ADDENDUM

Trials@uspto.gov
571-272-7822

Paper 80
Entered: June 2, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

ACHATES REFERENCE PUBLISHING, INC.
Patent Owner

Case IPR2013-00081
Patent 5,982,889

Before HOWARD B. BLANKENSHIP, JUSTIN T. ARBES, and GREGG I. ANDERSON, *Administrative Patent Judges.*

ARBES, *Administrative Patent Judge.*

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

Petitioner Apple Inc. ("Apple") filed a Petition (Paper 1) ("Pet.) seeking *inter partes* review of claims 1-4 of U.S. Patent No. 5,982,889 ("the '889 patent") pursuant to 35 U.S.C. §§ 311-19. On June 3, 2013, we instituted an *inter partes* review of claims 1-4 on four grounds of unpatentability (Paper 21) ("Dec. on Inst.").

Patent Owner Achates Reference Publishing, Inc. ("Achates") filed a Patent Owner Response (Paper 36) ("PO Resp."), which included a statement of material facts. Apple filed a Reply (Paper 49) ("Pet. Reply") and a response (Paper 50) ("Pet. SOF Resp.") to the statement of material facts.

Achates filed a Motion to Exclude (Paper 57) ("Mot. to Exclude") certain testimony submitted by Apple in the proceeding. Apple filed an Opposition to the Motion to Exclude (Paper 61) ("Exclude Opp."), and Achates filed a Reply (Paper 62) ("Exclude Reply").

Apple filed a Motion for Observation (Paper 64) ("Obs.") on certain email communications between Achates' two declarants, Mr. Dmitry Radbel and Dr. Xin Wang. Achates filed a response (Paper 69) ("Obs. Resp."). Achates also filed a Motion to Seal (Paper 68) ("Mot. to Seal") the email communications, and Apple filed an opposition (Paper 74) ("Seal Opp.").

An oral hearing was held on February 26, 2014, and a transcript of the hearing is included in the record (Paper 79) ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(c). This final written decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons that follow, we determine that Apple has shown by a preponderance of the evidence that claims 1-4 of the '889 patent are unpatentable.

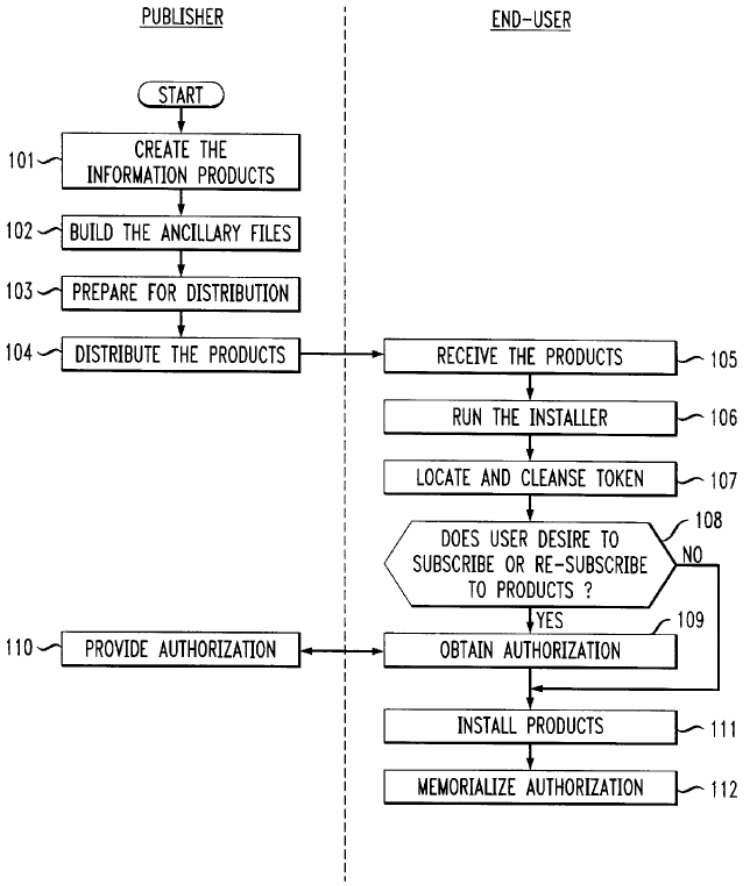
A. The '889 Patent

The '889 patent[1] relates to "distributing and installing computer programs and data." Ex. 1001, col. 1, ll. 6-9. The '889 patent describes a need in the art to prevent piracy of information products, such as, for example, when a user obtains a computer program improperly or when a user purchases one copy of a program and installs it on multiple computers without authorization. *Id*. at col. 1, ll. 12-60. The '889 patent discloses methods of "distributing one or more information products together . . . while reserving to the publisher the ability to control which products are actually installed on an end-user's computer." *Id*. at col. 1, l. 66-col. 2, l. 4.

[1] U.S. Patent No. 6,173,403 B1 ("the '403 patent"), a continuation-in-part of U.S. Patent Application No. 08/845,805, which issued as the '889 patent, is the subject of related Case IPR2013-00080.

Figure 1 of the '889 patent, reproduced below, depicts the interaction between a publisher and end-user (e.g., an individual purchasing a piece of software).

FIG. 1



As shown in Figure 1, in steps 101-102, the publisher creates a set of information products and other files. *Id*. at col. 3, ll. 34-40; col. 5, ll. 45-50. The '889 patent describes a "plurality of web pages that constitute some of the legislative, administrative and judicial materials associated with patent law," where the web pages include hyperlinks to each other, as an exemplary information product. *Id*. at col. 2, l. 64-col. 3, l. 1; col. 4, ll. 9-15. In step 103, the publisher encrypts the information products with a string as the

encryption key. *Id*. at col. 8, ll. 36-45. In step 104, the information products are distributed to the end-user (e.g., on a CD-ROM or electronically over the Internet) along with an "installer" program that runs on the end-user's computer and allows the publisher to "control how and under what circumstances the information products are installed on the end-user's computer." *Id*. at col. 2, ll. 39-48; col. 8, l. 65-col. 9, l. 3. The installer knows the cryptosystem and key for decrypting the information products. *Id*. at col. 8, ll. 57-59.

In steps 105-106, the end-user receives the information products and runs the installer. *Id*. at col. 9, ll. 4-15. In step 107, the installer checks to see whether the end-user's computer has a previously-stored, encrypted "token" indicating that the publisher granted authorization earlier to install the information products (e.g., when an end-user has a subscription to receive multiple products over time). *Id*. at col. 9, ll. 16-31. In step 108, the end-user is asked whether he or she wants to subscribe to the information products. *Id*. at col. 10, ll. 56-62. If so, in steps 109-110, the end-user "acquires the installer[']s cooperation to decrypt and install the respective information products" by transmitting information to the publisher, receiving a "launch code" from the publisher in response, and entering the "launch code" into the installer. *Id*. at col. 10, l. 63-col. 11, l. 9; Fig. 4. Specifically, the end-user contacts the publisher (e.g., via telephone or the Internet) and provides (1) the end-user's name and address; (2) the end-user's method of payment; (3) the name of the requested information products; and (4) a serial number R generated by the installer. *Id*. at col. 11, ll. 10-33.

After verifying the payment, the publisher provides to the end-user a "launch code" comprising "(1) a[n] authentication code; (2) an indication of

the name of the end-user; (3) a list of the information products to which the end-user has been granted access; and (4) an indication of when the authorization for each information product expires," encrypted using R as the key. *Id*. at col. 11, ll. 34-49. The end-user enters the launch code into the installer, and the installer decrypts the launch code using R as the key to extract the authentication code contained therein. *Id*. at col. 11, ll. 47-54. If the authentication code matches what the installer expects, the launch code is authentic. *Id*. at col. 11, ll. 50-65; col. 12, ll. 25-49. The information products can be installed in step 111 and, if necessary, the encrypted "token" on the end-user's computer is updated in step 112 (the "token" contains the same four pieces of information as the launch code). *Id*.; col. 9, ll. 40-47. By generating a new R each time the installer requests a launch code, the disclosed method "prevent[s] the end-user from using a single launch code to install the information products on multiple computers." *Id*. at col. 11, l. 66-col. 12, l. 2.

B. Illustrative Claim

Claim 1 of the '889 patent is the only independent claim at issue:

> 1. A method comprising the steps of:
>
> generating a string, R;
>
> encrypting a first authentication code, an indicium of an end-user's identity, an indicium of a first information product, and an indicium of a second information product with said string, R, as the key to create a launch code;
>
> decrypting said launch code with said string, R, to recover said authentication code, said indicium of said end-user's identity, said indicium of said first information product and said indicium of said second information product; and

> installing said first information product and said second information product onto a computer associated with said end-user.

C. Prior Art

The pending grounds of unpatentability in this *inter partes* review are based on the following prior art:

> 1. U.S. Patent No. 5,864,620, filed Apr. 24, 1996, issued Jan. 26, 1999 ("Pettitt") (Ex. 1006);
>
> 2. U.S. Patent No. 5,933,497, filed Jan. 29, 1993, issued Aug. 3, 1999 ("Beetcher") (Ex. 1007) (claims priority to U.S. Patent Application No. 07/629,295, filed Dec. 14, 1990); and
>
> 3. U.S. Patent No. 5,949,876, filed Jan. 8, 1997, issued Sept. 7, 1999 ("Ginter") (Ex. 1005) (claims priority to U.S. Patent Application No. 08/388,107, filed Feb. 13, 1995).

D. Pending Grounds of Unpatentability

This *inter partes* review involves the following grounds of unpatentability:

Reference(s)	Basis	Claims
Ginter	35 U.S.C. § 102(e)	1-3
Pettitt and Beetcher	35 U.S.C. § 103(a)	1-4
Beetcher and Ginter	35 U.S.C. § 103(a)	1-4[2]

[2] As explained below, Apple asserts that claim 4 is unpatentable based on the combination of Beetcher and Ginter in two respects: one relying on Beetcher as teaching the majority of the claim limitations, and one relying on Ginter as teaching the majority of the claim limitations. *See infra* Section II.G.2. A trial was instituted on both bases. *See* Dec. on Inst. 22-23, 30.

II. ANALYSIS

A. Claim Interpretation

In the Decision on Institution, we interpreted various claim terms of the '889 patent as follows:

Term	Interpretation
"authentication code" (claim 1)	a code for authenticating data
"installing" (claim 1)	placing in a position so as to be ready for use
"launch code" (claim 1)	password
"token" (claim 2)	a data structure indicating that an end-user's computer is granted access to certain information products

Dec. on Inst. 7-11. The parties agree with these interpretations, *see* PO Resp. 1, and we incorporate our previous analysis for purposes of this decision.

B. Section 315(b)

Achates argues in its Patent Owner Response that Apple's Petition is time-barred under 35 U.S.C. § 315(b), which provides that an *inter partes* review may not be instituted based on a petition "filed more than 1 year after the date on which the petitioner, real party in interest, or privy of the petitioner is served with a complaint alleging infringement of the patent." PO Resp. 44-51. Achates contends that QuickOffice, Inc. ("QuickOffice"), one of Apple's co-defendants in *Achates Reference Publishing, Inc. v. Symantec Corp.*, Case No. 2:11-cv-00294-JRG-RSP (E.D. Tex.) ("the related litigation"), was served with a complaint alleging infringement of the

'889 patent on June 20, 2011—more than one year before December 14, 2012, the filing date of the Petition in this proceeding. PO Resp. 45, 56. Achates made a substantially similar argument in its Preliminary Response, and we concluded that the Petition was not time-barred. *See* Paper 14 at 6-21; Dec. on Inst. 12-18. We reach the same conclusion now.[3]

Whether a non-party is a "privy" for purposes of an *inter partes* review proceeding is a "highly fact-dependent question" that takes into account how courts generally have used the term to "describe relationships and considerations sufficient to justify applying conventional principles of estoppel and preclusion." Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,759 (Aug. 14, 2012) ("Trial Practice Guide"). Whether parties are in privity depends on whether the relationship between a party and its alleged privy is "sufficiently close such that both should be bound by the trial outcome and related estoppels." *Id*. Depending on the circumstances, a number of factors may be relevant to the analysis, including whether the non-party "exercised or could have exercised control over a party's participation in a proceeding" or whether the non-party is responsible for funding and directing the proceeding. *Id*. at 48,759-60. We also find guidance in the Supreme Court's decision in *Taylor v. Sturgell*, 553 U.S. 880 (2008), which sets forth the general rule under federal common law that a person not a party to a lawsuit is not bound by a judgment in that suit, subject to certain exceptions, including the following:

> [N]onparty preclusion may be justified based on a variety of pre-existing "substantive legal relationship[s]" between the person to be bound and a party to the judgment. Qualifying

[3] Also, in an earlier Order, we denied Achates's request for additional discovery on the Section 315(b) issue. Paper 17.

> relationships include, but are not limited to, preceding and succeeding owners of property, bailee and bailor, and assignee and assignor. These exceptions originated "as much from the needs of property law as from the values of preclusion by judgment."

553 U.S. at 894 (citations omitted); *see* Trial Practice Guide at 48,759 (citing *Taylor*).

Achates contends that QuickOffice had a pre-existing substantive legal relationship with Apple and, therefore, is a privy of Apple under *Taylor*. PO Resp. 44-51. In support of its position, Achates cites a publicly available software development kit (SDK) agreement that Apple allegedly enters into with iPhone application developers like QuickOffice. *Id*. at 46-47. The SDK agreement includes a clause requiring the developer to indemnify Apple for third party patent infringement claims:

> To the extent permitted by law, *You agree to indemnify, defend and hold harmless Apple, its directors, officers, employees, independent contractors and agents (each an "Apple Indemnified Party") from any and all claims, losses, liabilities, damages, expenses and costs (including without limitation attorneys fees and court costs) (collectively "Losses") incurred by an Apple Indemnified Party as a result of* Your breach of this Agreement, a breach of any certification, covenant, representation or warranty made by You in this Agreement, *any claims that Your Applications violate or infringe any third party intellectual property* or proprietary rights, or otherwise related to or arising from Your use of the SDK, Your Application(s) or Your development of Applications.
>
> . . .
>
> *In no event may You enter into any settlement or like agreement with a third party that affects Apple's rights or binds Apple in any way, without the prior written consent of Apple.*

Ex. 2006 § 6 (emphasis added). According to Achates, the fact that co-defendant QuickOffice would be obligated to indemnify Apple for infringement claims against the "same accused instrumentality" (i.e., a QuickOffice application), and would be prevented from settling in the litigation without Apple's consent, means that QuickOffice and Apple are in privity with each other. PO Resp. 44-51. Apple acknowledges that it entered into "at least one form of an agreement related to app[lication] development with [QuickOffice]," but does not admit that the agreement included the indemnification provision cited by Achates. Pet. SOF Resp. ¶¶ 129-30.

We first note that Achates provides no evidence that QuickOffice had any role in the filing or funding of the Petition in this proceeding, or that QuickOffice exercised control or could have exercised control over Apple's participation in this proceeding. *See* Trial Practice Guide, 77 Fed. Reg. at 48,759. Achates's sole evidence is the indemnification language in the SDK agreement and the fact that Apple and QuickOffice were co-defendants.

Even assuming that the specific indemnification provision of the SDK agreement applies to QuickOffice (and Achates has not shown that it does), we are not persuaded that the provision is indicative of QuickOffice being a privy of Apple. The agreement does not give the developer the right to intervene or control Apple's defense to any charge of patent infringement, nor has Achates argued that to be the case for QuickOffice in the related litigation. Notably, indemnification is not one of the "substantive legal relationships" cited in *Taylor* (e.g., assignee-assignor), and is significantly different from those relationships, which involve successive interests in the same property.

Further, as Apple points out, Achates's actions in the related litigation refute its allegations of privity. *See* Pet. Reply 14. Achates accuses Apple of infringing the '889 patent based on Apple's own actions as well as those of QuickOffice, and likewise accused QuickOffice of infringement based on activities relating to the Apple App Store as well as other systems (e.g., the Amazon Appstore for Android). *See* Ex. 1037 ¶¶ 51-52; Ex. 1038 at 84-90. Achates also is continuing to assert the '889 patent against Apple in the related litigation even after settling with the co-defendant application developers, including QuickOffice. *See* PO Resp. 57. Thus, at least according to Achates, there is a distinct basis for liability against Apple, different from that against the developers. As such, it does not appear that Apple would be estopped by any judgment against the developers. For instance, even if a judgment were obtained against one or more of the developers, Apple would still be exposed to an adverse judgment based on its own actions and would assert its own defenses independent of the developers. This further indicates that the relationship between Apple and the developers, such as QuickOffice, is not of the type that would make the developers privies of Apple.

We are not persuaded that the Petition is time-barred under Section 315(b) on the basis that QuickOffice is a privy of Apple.

C. Credibility of Mr. Schneier

As an initial matter, Achates in its Patent Owner Response challenges the credibility of Apple's declarant, Bruce Schneier. PO Resp. 51-55. Mr. Schneier provided testimony regarding the '889 patent and the prior art

in a declaration submitted with Apple's Petition. Ex. 1003.[4] Achates argues that Mr. Schneier is not credible for two reasons. First, Mr. Schneier billed Apple for less than 45 hours of work, which is "nowhere near enough time to read and analyze all of the references cited in his declarations at the level of diligence that this proceeding requires," according to Achates. PO Resp. 51-53. For instance, Achates points to the size of Ginter (324 pages) and the declarations themselves (931 numbered paragraphs) to argue that Mr. Schneier "could not have performed his obligation to this matter conscientiously in the time spent." *Id*. Achates's estimate of 45 hours, however, is based on an estimate from Mr. Schneier as to the total amount Mr. Schneier *billed* to Apple. Ex. 1045 at 63:15-24; *see* PO Resp. 52. Achates does not point to any statement from Mr. Schneier regarding the number of hours he actually spent reviewing the prior art and performing the analysis in his declaration. Mr. Schneier testified that he read the prior art references at issue (Ginter, Pettitt, and Beetcher) multiple times and fully understood them. Ex. 1045 at 76:16-22, 77:21-78:5. Moreover, Achates's contention is not that Mr. Schneier lacks knowledge of the prior art or did not in fact perform the analysis in his declaration—just that Mr. Schneier did not spend sufficient time on the matter. We decline Achates's invitation to give Mr. Schneier's testimony less weight on that basis.

[4] Apple submitted its Petition, and Exhibits 1003 and 1041 (declarations from Mr. Schneier regarding the '889 patent and related '403 patent), on December 14, 2012. In response to an instruction from Board administrative staff that documents should be in portrait rather than landscape orientation, Apple submitted revised copies on December 17, 2012, also numbered as Exhibits 1003 and 1041. *See* Paper 5. To ensure the clarity of the record, the original versions filed on December 14, 2012 will be expunged.

Second, Achates argues that Mr. Schneier has "hostility towards the patent system" and is a member of the Electronic Frontier Foundation (EFF), which shows a "level[] of bias that should be more than sufficient to raise concerns about his qualifications to serve as an unbiased technology expert." PO Resp. 53-55 (citing a book co-authored by Mr. Schneier, Ex. 2016, and various EFF web pages, Exs. 2017-2020). We have reviewed Mr. Schneier's curriculum vitae (Exhibit 1004) and find that he is well qualified to testify regarding the matters addressed in his declaration (Exhibit 1003). Indeed, Achates's declarant, Mr. Radbel, testified that Mr. Schneier is a "top cryptologist" and has a "great reputation as a cryptologist." Ex. 2032 at 167:9-25. As explained herein, we find Mr. Schneier's testimony persuasive and give it substantial weight. We do not give it less weight based on a purported bias against patents in general.

D. Level of Ordinary Skill in the Art

In its Petition, Apple contends that a person of ordinary skill in the art at the time when the application that issued as the '889 patent was filed (April 1997) would have had "extensive familiarity with cryptographic techniques published in the literature and known in the field," and "would have gained this level of familiarity through graduate level studies in mathematics, engineering or computer science, or through work experience in academia (either as a professor or a graduate student), for a technology company or for a government," relying on the testimony of Mr. Schneier. Pet. 4 (citing Ex. 1003 ¶¶ 36-38). Achates does not dispute this argument in

its Patent Owner Response.[5] Mr. Radbel, however, concludes that a person of ordinary skill in the art would have had "the ability to select and make use of well-known cryptographic techniques at a high level," but not "comprehensive knowledge of cryptography, including Mr. Schneier's book on the subject." Ex. 2013 ¶¶ 17, 19. Mr. Radbel further testifies that a person of ordinary skill in the art would have had "an undergraduate degree in engineering or computer science plus two years of experience in software engineering," but not necessarily "graduate level training." *Id.* Dr. Wang agrees with Mr. Radbel's assessment of the level of ordinary skill. Ex. 2014 ¶ 8.

The parties' declarants appear to agree that the person of ordinary skill in the art would have been familiar with the basic cryptographic techniques of the time, but dispute the depth of that knowledge. A skilled artisan would have been aware of basic cryptographic techniques and also the predominant literature on cryptography of the time. *See In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) ("The person of ordinary skill in the art is a hypothetical person who is presumed to know the relevant prior art."). As to that person's level of education or equivalent experience, we are persuaded that Mr. Radbel understates the appropriate level of skill. The '889 patent describes various problems with software piracy and various technical solutions to such problems. Ex. 1001, col. 1, ll. 12-60. It also

[5] Achates argued in its Preliminary Response that "the proper level of skill should be a person with at least five years of experience and[/]or academic training in professional software development having experience with client-server software and operating systems, and at least a basic working knowledge of computer security and cryptography." Paper 14 at 23.

assumes a fairly deep knowledge of encryption, decryption, and the use of keys for performing those functions. *See id*. at col. 8, l. 35-col. 12, l. 49. Contrary to Mr. Radbel's assertion that a person of ordinary skill only would have needed a "high level" knowledge of cryptographic techniques, sufficient, for example, to call software routines "without necessarily understanding how such routines work," *see* Ex. 2013 ¶ 17, a skilled artisan would need some knowledge of how the cryptographic techniques work to choose the appropriate techniques and properly use them. We also take into account the sophistication of the technology at the time, as exemplified by the prior art references of record and Mr. Schneier's book from 1996 (Exhibit 1024). Based on all of the evidence, we conclude that a person of ordinary skill in the art at the time of the '889 patent would have been familiar with the basic cryptographic techniques and literature of the time, and would have had some graduate-level or equivalent experience working with such techniques.

E. Ground Based on Ginter

With respect to the alleged ground of unpatentability based on Ginter, we have reviewed Apple's Petition, Achates's Patent Owner Response, and Apple's Reply, as well as the evidence discussed in each of those papers. We are persuaded, by a preponderance of the evidence, that claims 1-3 are anticipated by Ginter under 35 U.S.C. § 102(e).

1. Ginter

Ginter discloses computer systems providing a "distributed virtual distribution environment (VDE)" that "help[s] to ensure that information is

accessed and used only in authorized ways." Ex. 1005, Abstract. Electronic content is stored in "objects" (also called "containers") for distribution to users, and access to the content is regulated via a permissions record (PERC) associated with the content and provided to the user (separately or with the object). *Id*. at col. 13, l. 46-col. 14, l. 20; col. 58, l. 61-col. 59, l. 11; Fig. 5A; col. 147, ll. 33-59 ("no end user may use or access a VDE object unless a permissions record 808 has been delivered to the end user"). PERC 808 "specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active." *Id*. at col. 58, l. 67-col. 59, l. 5. "For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content." *Id*. at col. 59, ll. 5-7. For certain types of objects, the PERC is encrypted along with the object using a symmetric key and later decrypted on the user's machine. *Id*. at col. 199, ll. 1-6; col. 129, ll. 50-54; col. 133, ll. 50-53; col. 208, l. 65-col. 209, l. 20. Ginter discloses that the PERC can contain an "Object ID" that identifies the VDE object, as well as multiple "key blocks" that store decryption keys utilized to access content in "data blocks" within the object. *Id*. at col. 127, l. 45-col. 128, l. 2; col. 151, ll. 9-35; Fig. 26A. Ginter also discloses the use of a "validation tag" for "confirming the identity and correctness of received, VDE protected, information," and a "digital signature" to be verified against an expected digital signature. *Id*. at col. 12, ll. 27-33; col. 151, ll. 9-35; col. 215, ll. 7-63.

2. Claims 1-3 are Anticipated by Ginter

Ginter discloses generating a "string, R" (the symmetric key), encrypting an "indicium of an end-user's identity" (the PERC specifying "who" can open the container, use the object's contents, etc.) and an indicium of a first "information product" (the Object ID or key block) to create the PERC, decrypting the PERC, and installing the first information product onto the end-user's computer, as recited in claim 1. *See* Pet. 24-30; Ex. 1003 ¶¶ 121-75.

Achates does not argue these limitations, but makes three arguments regarding the remaining limitations of claim 1. First, Achates argues that Ginter does not disclose "decrypting said launch code . . . to recover said authentication code," as recited in claim 1. PO Resp. 4-9. Achates contends that the first item in Ginter identified by Apple as an "authentication code" (the digital signature) is not contained in the PERC and, therefore, the PERC cannot be decrypted to recover it, and the second item identified by Apple (the validation tag) is not an "authentication code." *Id*. at 5-9; *see* Pet. 25-26; Ex. 1003 ¶ 141. Ginter expressly discloses a PERC including a digital signature. Ex. 1005, col. 12, ll. 27-33. Figure 75D depicts user rights table (URT) 3160 as including a digital signature, and Ginter states that URT 3160 "may itself be a PERC 808." *Id*. at col. 248, ll. 36-38, Fig. 75D. Thus, Achates's factual assertion that the PERC in Ginter lacks a digital signature is not correct. *See* Tr. 47:24-48:5 (acknowledging the description of Figure 75D in Ginter). Mr. Radbel also acknowledged that the PERC could have a

digital signature in the "particular construct" shown in Figure 75D. Ex. 2032 at 279:14-18.[6]

Second, Achates contends that the PERC in Ginter is not a "launch code" comprising indicia of multiple "information product[s]," as recited in claim 1. PO Resp. 9-15 (citing Ex. 2013 ¶¶ 55-64). Apple's position is that the Object ID and key blocks in the PERC both satisfy the "indici[a]" limitations of claim 1. Pet. 25-26. As to the Object ID, Achates contends that (1) Object ID field 940 in Ginter is a single field that identifies the VDE object and, therefore, cannot be both an indicium of a first information product and an indicium of a second information product, (2) Object ID field 940 identifies the "totality" of elements in the VDE object container, not "just" information content 304, and (3) Object ID field 940 has the same datum regardless of whether the container's content is changed or deleted, which shows that Object ID field 940 is not an "indicium" of a particular information product. PO Resp. 9-13. As to the key blocks, Achates argues that (1) the VDE accesses the datum in the key block to use as a key to decrypt the corresponding data blocks, not "as a pointer to—or indicium of—the data block," and (2) Ginter permits two key blocks to have the same key, which shows that the key block is not an "indicium" of a particular information product. *Id*. at 13-15.

Achates's arguments are not persuasive, as they are based on two incorrect premises. *See* Pet. Reply 3-4. The first incorrect premise is that an "indicium" of an information product can *only* identify content within a file

[6] Because we agree with Apple as to the PERC in Ginter having a digital signature, we need not determine whether the validation tag also is an "authentication code."

and must uniquely identify *only one* information product. *See id*. There is no prohibition in claim 1 on the indicium indicating other things, and the indicium need not be a "pointer." *See* Ex. 2032 at 304:18-305:2 (Mr. Radbel stating that he does not "consider indicium to be a pointer"). The only requirement is that it be an "indicium," or "indication," of an information product. Mr. Radbel acknowledged that the Object ID in Ginter is used to find the correct content, Ex. 2031 at 45:12-17, and the key blocks are associated with and used to access the data in the correct data block, Ex. 1005 at 127:45-128:2. Achates's second incorrect premise is that each information product must have a unique indicium. Again, claim 1 does not require that the particular content of the "indici[a]" be different from each other. We are persuaded by Mr. Schneier's testimony that the key blocks and Object ID in Ginter are "indici[a]" of information products. *See* Pet. 25; Ex. 1003 ¶¶ 146-51, 168.

Third, Achates is incorrect in its assertion that Apple's analysis is based on "disjoint parts of Ginter without regard to their relationship." PO Resp. 3-4. Achates does not develop this argument with respect to the particular limitations of claims 1-3 or explain sufficiently why the particular portions of Ginter cited for the limitations of these claims relate to different embodiments, rather than the same preferred embodiment.

We are persuaded, by a preponderance of the evidence, that claim 1, as well as dependent claims 2 and 3, which Achates does not argue separately in its Patent Owner Response, are anticipated by Ginter.

3. Conclusion

Based on the record evidence, in light of the arguments presented, Apple has shown, by a preponderance of the evidence, that claims 1-3 are anticipated by Ginter.

F. Ground Based on Pettitt

With respect to the alleged ground of unpatentability based on Pettitt, we have reviewed Apple's Petition, Achates's Patent Owner Response, and Apple's Reply, as well as the evidence discussed in each of those papers. We are persuaded, by a preponderance of the evidence, that claims 1-4 are unpatentable over Pettitt and Beetcher under 35 U.S.C. § 103(a).

1. Pettitt

Pettitt discloses a system for "controlling distribution of software in a multitiered distribution chain" and "distinguishing authorized users from unauthorized users." Ex. 1006, col. 1, ll. 7-10.

Figure 2 of Pettitt is reproduced below.

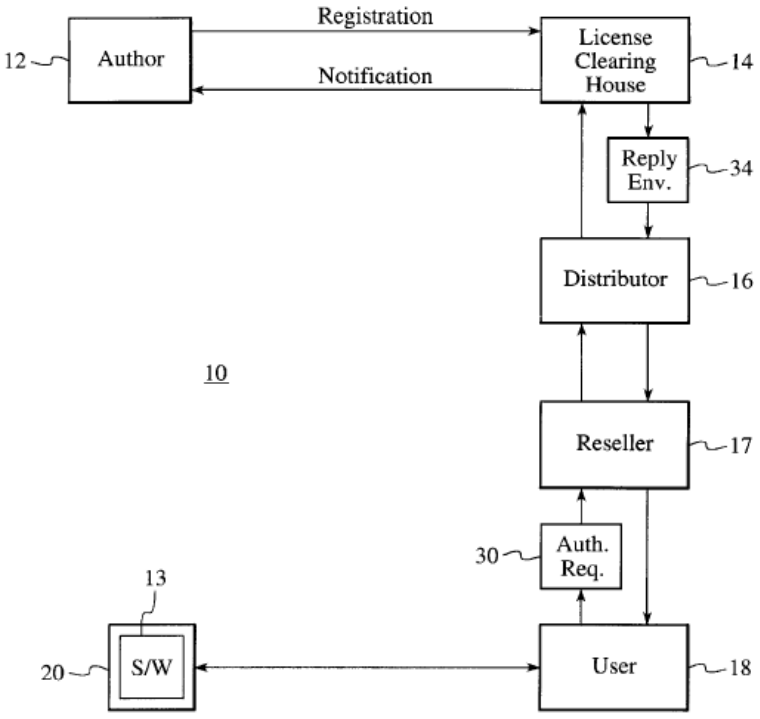


FIG. 2

Figure 2 depicts the entities involved in providing software 13: author 12, license clearing house (LCH) 14, distributor 16, reseller 17, and user 18. Software 13 is packed into a digital shipping container 20, encrypted with a master key, and provided to user 18 (e.g., sold by reseller 17 to the public). *Id*. at col. 3, ll. 28-56. To purchase a license and unlock the container, user 18 sends authorization request 30, which includes information identifying the software, user, and desired method of payment. *Id*. at col. 4, ll. 10-19. The distribution entities communicate with each other to validate the user's payment and authorize the transaction. *Id*. at col. 4, ll. 20-62. If authorized, LCH 14 creates a reply envelope 34 including:

1. information identifying the software,
2. information identifying the user,
3. the digital signature of the reseller,

4. the digital signature of the distributor,

5. a master key that unlocks the software container 20 (if the transaction has been authorized), and

6. a digital authorization certificate.

Id. at col. 4, l. 63-col. 5, l. 5.

LCH 14 encrypts the contents of the reply envelope with the reseller's public key and "digitally signs the envelope with the signature of LCH 14 by hashing the contents of the reply envelope and encrypting the result of the hash with the LCH's private key." *Id*. at col. 5, ll. 14-24. LCH 14 then sends the reply envelope back through the distribution chain. *Id*. at col. 5, ll. 24-28. Reseller 17 authenticates the digital signature, decrypts the reply envelope using the reseller's public key, and sends the contents of the reply envelope to user 18. *Id*. at col. 5, ll. 45-55. User 18 then "uses the authorization certificate and the master key to unlock the software container 20 and install the software." *Id*. at col. 5, ll. 56-63. Because the digital authorization certificate is derived from the user's information and, therefore, is different for each user, possession of the digital authorization certificate is "the user's proof of purchase, and proof that s/he is an authorized user." *Id*. at col. 5, ll. 58-63.

2. Claims 1-4 are Unpatentable Over Pettitt and Beetcher

Claim 1

Pettitt teaches generating a "string, R" (the reseller's public key), encrypting an "indicium of an end-user's identity" (information identifying the user) and an "indicium of a first information product" (information identifying the software) to create a "launch code" (the reply envelope), decrypting the "launch code," and installing the first information product

onto the end-user's computer, as recited in claim 1. *See* Pet. 33-35. Apple relies on Beetcher for the "second information product" limitations of claim 1, as Pettitt refers only to a user purchasing a single piece of software. *See id*. at 36-38; Ex. 1006, col. 2, l. 59-col. 3, l. 1; col. 4, ll. 8-19.

In its Patent Owner Response, Achates makes two arguments regarding claim 1. First, Achates argues that Pettitt does not teach "decrypting said launch code . . . to recover said authentication code," as recited in claim 1. PO Resp. 19-27. Achates contends that Pettitt's LCH digital signature and digital authorization certificate, each cited by Apple in the Petition as an "authentication code," are not authentication codes recovered by decrypting the reply envelope in Pettitt. *Id*. As to the digital authorization certificate, Achates acknowledges that the certificate is part of the reply envelope and that the "reseller does *recover* the certificate by decrypting the encrypted reply envelope." *Id*. at 23. Achates's position, however, is that the digital authorization certificate is not an "authentication code" for two reasons: (1) the digital authorization certificate is used to unlock and install the software and distinguish authorized from unauthorized users, not to authenticate data, and (2) the digital authorization certificate is not used to authenticate the reply envelope because the reseller authenticates the encrypted reply envelope with the LCH digital signature before the reseller decrypts the reply envelope. *Id*. at 23-27. In support of its position, Achates relies on Dr. Wang, who explains why he believes that "Pettitt's digital authorization certificate is not an authentication code." Ex. 2014 ¶¶ 19-23.

We are persuaded that Pettitt's decryption of the reply envelope to recover the digital authorization certificate constitutes "decrypting said

launch code . . . to recover said authentication code," as recited in claim 1. *See* Pet. 34; Ex. 1003 ¶¶ 207-208. As explained above, we interpret "authentication code" to mean "a code for authenticating data." *See supra* Section II.A. The digital authorization certificate is generated by hashing the other five items identified in Pettitt as being part of the reply envelope and encrypting the result with the private key of the LCH. Ex. 1006, col. 5, ll. 6-8. Therefore, the digital authorization certificate is a digital signature, and a function of a digital signature is to authenticate data, as Dr. Wang agrees. *See* Ex. 2034 at 254:15-21, 257:17-23. Pettitt specifies that the digital authorization certificate is "use[d]" to unlock the software container and install the software. Ex. 1006, col. 5, ll. 56-58. Specifically, the user would validate the digital authorization certificate by decrypting the originally encrypted hash (e.g., with the LCH's public key), generating a new hash from the same five elements used to create the original hash, and comparing the new and original hashes. *See* Pet. Reply 6; Ex. 2034 at 193:3-194:8, 263:10-15. Thus, the digital authorization certificate authenticates the data that has been "digitally signed" with it. Further, as Achates acknowledges, the digital authorization certificate is part of the encrypted reply envelope, and is recovered when the reply envelope is decrypted. *See* Ex. 1006, col. 4, l. 63-col. 5, l. 8; col. 5, ll. 51-63 ("reseller 17 decrypts the reply envelope . . . and passes the contents onto the user 18"); PO Resp. 23. Therefore, we are persuaded that Pettitt teaches "decrypting said launch code . . . to recover said authentication code," as recited in claim 1.[7]

[7] Because we agree with Apple that the digital authorization certificate in Pettitt is an "authentication code" recovered by the decryption of a launch

We also note that, in its Motion for Observation, Apple cites an email communication between Dr. Wang and Mr. Radbel where Dr. Wang stated: "I am still struggling with their statements like the authorization certificate does not authenticate data. . . . I thought we agreed during the call that we are not going to use this line of argument." Obs. 1 (citing Ex. 1067 at 1). Although the specific "statements" referenced in the email are unknown, we agree with Apple that Dr. Wang's statement that he was "struggling" with "statements like the authorization certificate does not authenticate data" is inconsistent with his later opinion in his declaration that "a person of ordinary skill in the art would not consider the digital authorization certificate to be . . . a code for authenticating data." *See id*.; Ex. 2014 ¶¶ 22-23. For this and the other reasons explained above, we find Mr. Schneier's testimony to be more credible than that of Dr. Wang.

Second, Achates argues that Pettitt and Beetcher do not teach the limitations of claim 1 pertaining to multiple "indici[a]"—namely, decrypting a launch code to recover indicia of first and second information products, and installing the first and second information products. PO Resp. 27-32. According to Achates, Mr. Schneier provides "no reason" why a skilled artisan would modify Pettitt's reply envelope to be "capable of authorizing the installation of multiple information products." *Id*. at 28.

We first note that claim 1 does not recite "authorizing" the installation of any information products. The claim only recites "decrypting" the launch code to recover the indicia of the first and second information products, and "installing said first information product and said second information

---

code, as recited in claim 1, we need not determine whether the LCH digital signature also is an "authentication code."

product onto a computer associated with said end-user." Moreover, we disagree that Mr. Schneier gives "no reason" for the proposed combination. Mr. Schneier testifies as follows:

> I also believe that including more specific indications of more than one information product in the reply envelope of Pettitt would have been obvious to a person of ordinary skill in the art in 1997 because the inclusion of multiple such indicia was well known at the time and well within the skill of the art.
>
> *A person of ordinary skill in the art also would have had good reasons to include a list of multiple indicia of information products in the same launch code, as doing so would more efficiently identify multiple information products for which the end-user was licensed.*
>
> For example, . . . Beetcher explains that multiple software modules may be placed on a single distribution medium, and "[e]ach customer will receive a unique entitlement key enabling that customer to run only those software modules to which he is licensed."
>
> In addition, a person of ordinary skill would have recognized that the Pettitt scheme could have been easily extended to authorize multiple software products. This could have been done, for example, by including multiple "master keys" and/or indicia corresponding to the different software products within the reply envelope sent by the reseller. *Such master keys and indicia would be used in the same way as in the example in the patent, which sends a master key for one software product (e.g., it is used to unlock the software container if the transaction has been authorized).* Extending Pettitt to include multiple indicia of software products, thus, would have been an obvious alteration of the Pettitt scheme to a person of ordinary skill in the art in April of 1997.

Ex. 1003 ¶¶ 218-21 (citations omitted, emphasis added); *see* Pet. 36-38. We find Mr. Schneier's analysis supported by the disclosures of the references and persuasive. In addition, Dr. Wang acknowledges that "Pettitt

leaves the illegal copying problem to others, and Beetcher addresses this problem with runtime checks." Ex. 2014 ¶ 67; *see* Pet. Reply 6-7. Thus, Dr. Wang's own analysis indicates a reason why a skilled artisan would have looked to Beetcher to provide something that the Pettitt system lacks.

Achates also disputes Mr. Schneier's conclusion that if the Pettitt system were modified to handle multiple software products by including multiple master keys and indicia in the reply envelope, the master keys and indicia would be "used in the same way as in the example in the patent." PO Resp. 28-32 (citing Ex. 1003 ¶ 221). Achates contends that in Pettitt, there "can be" more than one distributor and more than one reseller, which may not carry all possible software products. *Id*. at 29. Achates then describes a hypothetical situation where a user requests one software product from one distributor/reseller pair and a second software product from a different distributor/reseller pair, and the LCH generates and transmits the reply envelope in response to the first request before the second request arrives. *Id*. at 29-30. Then, when the second request arrives, the LCH would create a new reply envelope, not a "consolidated reply envelope." *Id*. at 30. According to Achates, producing a consolidated reply envelope with master keys and indicia for multiple software products would require a "coordination function" at the LCH, as well as resolving various problems with transmission through the distribution chain and decryption of the reply envelope, all of which would amount to a "fundamental redesign" to the Pettitt system. *Id*. at 30-32.

We are not persuaded that a person of ordinary skill in the art would have been incapable of combining, or have had no reason to combine, the teachings of Pettitt and Beetcher in the manner alleged. Pettitt discloses a

multitiered software distribution system comprising "one or more distributors" and "one or more optional resellers." Ex. 1006, col. 3, ll. 28-32. Thus, the system may have only a single distributor and a single reseller (or even no reseller, as it is "optional"), and Achates's hypothetical situation is not guaranteed to occur. In addition, as Apple points out, Achates's hypothetical situation is merely attorney argument, unsupported by any testimony from Dr. Wang or Mr. Radbel or other evidence. *See* Pet. Reply 7-8. Dr. Wang also acknowledges that it would be possible to modify the Pettitt system to handle multiple information products. *See id.*; Ex. 2014 ¶ 67 ("if desired, Beetcher's prepared software could be distributed on Pettitt's system"); Ex. 2034 at 314:7-22. Thus, we are persuaded that combining the teachings of Pettitt and Beetcher is proper and that a person of ordinary skill in the art would have had reason to do so in the manner asserted by Apple and Mr. Schneier to arrive at the method of claim 1.

Claim 2

As to claim 2, Achates argues that a person of ordinary skill in the art would not have had reason to combine the teachings of Pettitt and Beetcher. PO Resp. 32-35. Claim 2 recites, *inter alia*, "creating a token," "encrypting said token," and "storing said encrypted token on said computer." As explained above, we interpret "token" to mean "a data structure indicating that an end-user's computer is granted access to certain information products." *See supra* Section II.A. In the Petition, Apple contends that when the reseller in Pettitt decrypts the reply envelope, it recreates the unencrypted reply envelope and sends the contents of the reply envelope (a "token") to the user. Pet. 37-38. The contents of the unencrypted reply

envelope (e.g., the master key and digital authorization certificate) are stored in the memory of the user's computer because they are used to unlock the software. *Id*. (citing Ex. 2003 ¶ 244). Apple further contends that although Pettitt does not teach encrypting the contents of the reply envelope in memory on the user's computer, doing so would have been an obvious, logical step based on Beetcher and would have been obvious given the fact that Pettitt teaches encrypting the reply envelope at various stages for security. *Id*. Mr. Schneier testifies that a "person of ordinary skill would recognize that encrypting a locally stored token would help protect the contents of the token from theft." Ex. 1003 ¶ 243 (citing Beetcher, Ex. 1007, col. 10, ll. 27-31, which teaches local storage of an encrypted entitlement key).

Achates contends that storing the encrypted reply envelope on the user's computer would not make sense because the encrypted reply envelope is encrypted with the public key of the reseller, so only the reseller, not the user, can decrypt it. PO Resp. 33. Pettitt, however, does not teach that the user ever receives the encrypted reply envelope. *See* Pet. Reply 8. Rather, the reseller decrypts the reply envelope and sends the *contents* to the user in unencrypted form. Ex. 1006, col. 5, ll. 51-55. Thus, it is the *contents* of the reply envelope that are stored on the user's computer, and we agree that it would have been obvious based on Beetcher to encrypt those contents when they are stored there.

Achates also asserts that because the reseller sends the master key (along with the other contents of the reply envelope) to the user, there is no reason for the user to back up the reply envelope locally once the user has used the master key to install the software. PO Resp. 33-34. In addition,

according to Achates, there is no need to save the encrypted reply envelope because the user can back up the software itself. *Id*. at 34-35. Again, Achates misstates Apple's position, focusing on the encrypted reply envelope rather than the *contents* of the envelope that the user receives. In Pettitt, all of the contents are sent to the user, the master key and digital authorization certificate are used to unlock and install the software, and thereafter "the possession of the authorization certificate is the user's proof of purchase, and proof that s/he is an authorized user." Ex. 1006, col. 5, ll. 56-63. Thus, there are reasons for the user in Pettitt to store the token, including the digital authorization certificate, locally—namely, to install and unlock the software and provide proof of purchase. *See* Pet. Reply 8-9; Ex. 1003 ¶¶ 240-44.

We also note that Achates does not dispute the underlying reasons provided by Mr. Schneier for why a person of ordinary skill in the art would have combined the teachings of Pettitt and Beetcher in the manner proposed. Mr. Schneier testifies that encrypting locally stored tokens was well known at the time and that a skilled artisan would have had reason to encrypt the token in Pettitt to ensure its security. Ex. 1003 ¶¶ 242-44. Dr. Wang agrees that it generally is a good practice to encrypt a file stored in nonvolatile storage to "protect the confidentiality of the file." Ex. 2035 at 395:3-15, 400:1-6. We give Mr. Schneier's analysis regarding the combination of Pettitt and Beetcher substantial weight, and conclude that Apple has shown "'some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'" *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417-18 (2007) (citation omitted).

We are persuaded, by a preponderance of the evidence, that claims 1 and 2, as well as dependent claims 3 and 4, which Achates does not argue separately in its Patent Owner Response, would have been obvious over Pettitt and Beetcher.

3. Conclusion

Based on the record evidence, in light of the arguments presented, Apple has shown, by a preponderance of the evidence, that claims 1-4 are unpatentable over Pettitt and Beetcher.

G. Ground Based on Beetcher

With respect to the alleged ground of unpatentability based on Beetcher, we have reviewed Apple's Petition, Achates's Patent Owner Response, and Apple's Reply, as well as the evidence discussed in each of those papers. We are persuaded, by a preponderance of the evidence, that claims 1-4 are unpatentable over Beetcher and Ginter under 35 U.S.C. § 103(a).

1. Beetcher

Beetcher discloses a system for "restricting the ability of a computer user to use licensed software in a manner inconsistent with the license." Ex. 1007, col. 1, ll. 9-12.

Figure 1 of Beetcher is reproduced below.

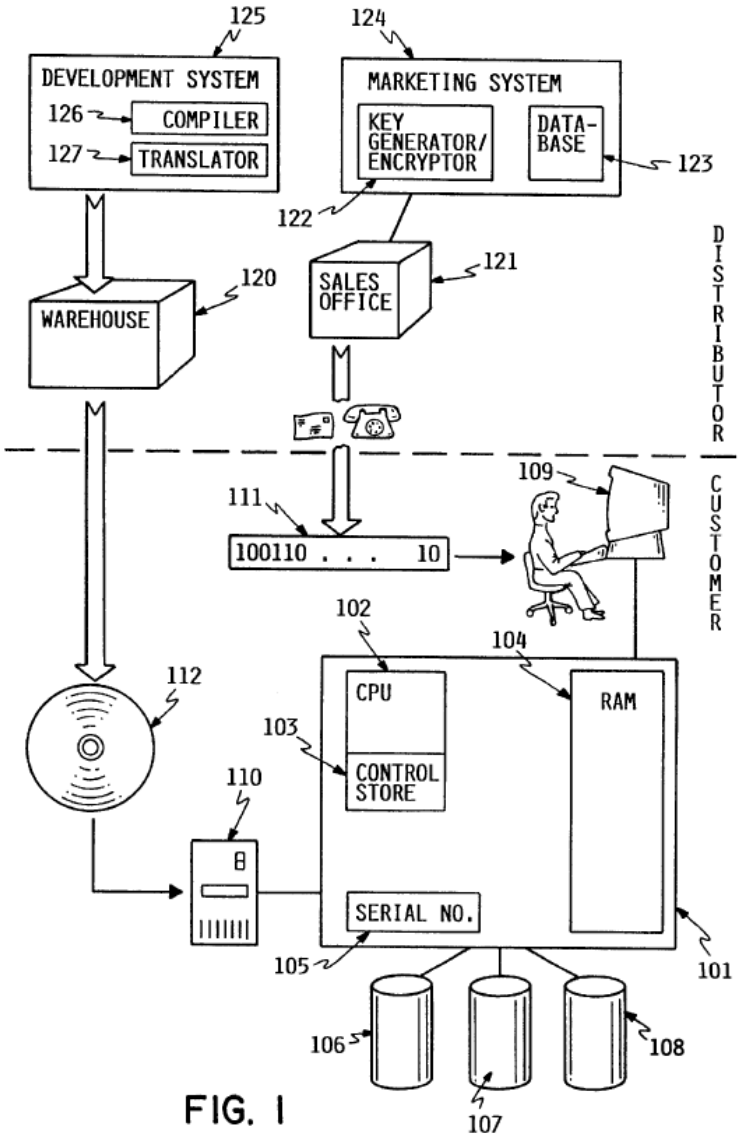


Figure 1 depicts various distributor and customer devices. The customer's computer has machine serial number 105. *Id*. at col. 5, ll. 17-23. A "generic set of software modules" stored on software media 112 is distributed to the customer separately from encrypted entitlement key 111, which "contains information enabling system 101 to determine which software modules are entitled to execute on it." *Id*. at col. 5, l. 65-col. 6, l. 7. The customer "load[s] the desired software modules from [software media 112 and] unit

110 into system 101, and store[s] the software modules on storage devices 106-108." *Id*. at col. 6, ll. 11-15. Entitlement key 111 includes certain information, such as software version field 202, machine serial number field 204, and product entitlement flags 205, "each corresponding to a product number" for a product that the customer may be authorized to use. *Id*. at col. 6, ll. 20-40; Fig. 2. Entitlement key 111 is encrypted using a machine key derived from machine serial number 105. *Id*. at col. 5, ll. 44-50; col. 9, ll. 55-60.

The customer receives encrypted entitlement key 111 and enters it into the computer. *Id*. at col. 9, ll. 51-52. The customer's computer then decodes encrypted entitlement key 111 using the machine key, stores the key in an encoded product key table, and stores the key and software version number in a product lock table. *Id*. at col. 6, l. 66-col. 7, l. 42. The encoded product key table and product lock table both are stored in random access memory (RAM), and the encoded product key table also is stored on a non-volatile storage device so that it can be recovered when the system is powered down and then re-initialized (i.e., the encoded product key table is persistent). *Id*. at col. 8, ll. 23-27, 43-46. Products are unlocked "on demand." *Id*. at col. 10, ll. 20-39. "Upon first execution of a previously unentitled software product," an unlock routine "fetches the encrypted entitlement key from the appropriate entry in [the] encoded product key table," "obtains the machine key," "decodes the entitlement key," and sets the product lock table accordingly if the entitlement key indicates that the user is entitled to use the software. *Id*. Upon subsequent executions of the software product, the system checks the product lock table to determine if the software is entitled to execute. *Id*. at col. 10, ll. 48-62.

2. Claims 1-4 are Unpatentable Over Beetcher and Ginter

Claims 1-3

Beetcher teaches generating a "string, R" (the machine key), encrypting an "indicium of an end-user's identity" (the machine serial number) and indicia of first and second "information product[s]" (the entitlement flags) to create a "launch code" (the entitlement key), decrypting the "launch code," and installing the first information product onto the end-user's computer, as recited in claim 1. *See* Pet. 8-11. Apple relies on Ginter's use of a digital signature for the "authentication code" limitations of claim 1 because the version number and machine serial number in Beetcher are used for purposes other than authenticating data. *See id*. at 10; Ex. 1007, col. 10, ll. 2-5, 56-60.

Achates makes three arguments regarding claim 1. First, Achates argues that Beetcher and Ginter do not teach "decrypting said launch code . . . to recover said authentication code," as recited in claim 1, because Ginter's permissions record (PERC) does not include a digital signature that can be recovered by decrypting the PERC. PO Resp. 36-40. We disagree, for the reasons explained above. *See supra* Section II.E.2. In addition, Achates's argument is directed to Ginter individually, but Apple's position regarding the recited "decrypting" step is premised on the combination of Beetcher and Ginter. Apple relies on Beetcher for the underlying teaching of decrypting an encrypted "launch code" (the entitlement key) to recover the software version number and machine serial number, and, because those two values are not authentication codes, relies on Ginter's teaching of a digital signature within an encrypted "launch code" (the PERC). *See* Pet. 13-14; Ex. 1003 ¶¶ 275-78. Given Ginter's teaching of a digital signature

within a PERC, Achates does not explain sufficiently why the substitution proposed by Apple would not result in the recited "decrypting" step. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references.").

Second, Achates argues that a person of ordinary skill in the art in 1997 would not have been motivated to include a digital signature in the entitlement key of Beetcher. PO Resp. 41-42. Achates contends that "public key cryptography was patented and the owner of the dominant patent was known to be litigious and the cost of its licenses high," citing a 1997 article regarding U.S. Patent No. 4,405,829. *Id*. (citing Ex. 2015). Achates also points to the following testimony from Mr. Schneier:

> Q. Does the fact that the digital signatures were all patents in the 1997 time frame create a motivation not to use digital signatures?
>
> A. Of course.

Ex. 1046 at 484:5-9.

We first note that Mr. Schneier later testified during redirect examination that he "may have made a mistake" regarding the testimony cited above because at least one digital signature algorithm of the time was in the public domain. *Id*. at 494:4-495:7. Moreover, even assuming that Achates is correct, Achates's argument is not that it would have been technically infeasible, or even technically difficult, for a person of ordinary skill in the art to use a digital signature in the context of Beetcher—just that the financial cost of doing so would have been high. We do not consider this to be a sufficient impediment to dissuade a skilled artisan from using

digital signatures. Indeed, Mr. Schneier testifies that digital signatures were "widely used in April 1997" in systems analogous to that of Beetcher, and provides detailed reasons why a person of ordinary skill in the art would have wanted to use a digital signature. *See* Ex. 1003 ¶¶ 275-78. Achates gives no basis for believing that testimony to be incorrect.

Third, relying on its other arguments addressed above, Achates argues that "[t]he nature and number of mistakes that [Apple] and Mr. Schneier make in their interpretation of the reference[s] betrays the[] fact that their propositions are based almost entirely on hindsight." PO Resp. 43. Achates further contends that a person of ordinary skill in the art would not have considered combining the references, citing Mr. Schneier's testimony that if he were tasked with solving the problem of small-scale software piracy in 1997, he would not have "bother[ed]" with Ginter. *Id*. at 43-44 (citing Ex. 1045 at 350:17-352:3, Ex. 1046 at 392:7-18). As explained above, we do not agree that Apple and Mr. Schneier misread Ginter or the other references, and are persuaded by Mr. Schneier's reasons as to why a person of ordinary skill in the art would have combined the teachings of Beetcher and Ginter. The cited portions of Mr. Schneier's testimony, which address how Mr. Schneier would have built a system and only show that he would not have looked to Ginter because it is "long" and "complex" and has many "unnecessary things," do not refute those reasons. *See* Ex. 1045 at 350:17-352:3; Ex. 1046 at 392:7-18.

We are persuaded, by a preponderance of the evidence, that claim 1, as well as dependent claims 2 and 3, which Achates does not argue separately in its Patent Owner Response, would have been obvious over Beetcher and Ginter.

Claim 4

As to claim 4, Apple argues that claim 4 is unpatentable based on the combination of Beetcher and Ginter in two respects. First, as explained above, Apple relies on Beetcher as teaching all limitations of claim 4 other than the "authentication code" limitations, and relies on Ginter as teaching the use of an "authentication code." Pet. 9-16. Second, Apple relies on Ginter as teaching all limitations of claim 4 other than "identical" strings R (for encrypting items to create a launch code) and T (for encrypting a token), and relies on Beetcher as teaching that limitation. *Id*. at 32-33. In the Decision on Institution, we determined that Apple had established a reasonable likelihood of prevailing based on Beetcher and Ginter for both reasons. Dec. on Inst. 22-23, 30. Achates does not argue claim 4 separately in its Patent Owner Response on either basis, instead relying on its arguments as to independent claim 1. *See* PO Resp. 15-16, 40, 42. After reviewing Apple's arguments in the Petition, and Mr. Schneier's supporting testimony, we are persuaded, by a preponderance of the evidence, that claim 4 would have been obvious over Beetcher and Ginter on both bases. *See* Pet. 9-16, 32-33; Ex. 1003 ¶¶ 194-99, 294-96, 298.

3. Conclusion

Based on the record evidence, in light of the arguments presented, Apple has shown, by a preponderance of the evidence, that claims 1-4 are unpatentable over Beetcher and Ginter.

H. Apple's Motion for Observation on Email Communications and Achates's Motion to Seal

Apple's Motion for Observation on email communications between Mr. Radbel and Dr. Wang pertains to certain statements the witnesses made regarding the term "authentication code" used in the claims (citing Exs. 1067, 1068). *See* Obs. 1-3. We have considered Apple's observations and Achates's response, and have addressed them above where relevant. *See supra* Section II.F.2; Obs. 1-3; Obs. Resp. 1-4.

Achates also moves to seal the email communications (Exhibits 1067 and 1068), as well as Apple's Motion for Observation (Paper 64)[8] and Achates's response (Paper 69). Mot. to Seal 2-4. In previous Orders, we ordered Achates to produce the emails, authorized Apple to file them as exhibits in this proceeding, and authorized Achates to file a motion to seal. *See* Papers 43, 52, 58, 63.

There is a strong public policy in favor of making information filed in an *inter partes* review open to the public, especially because the proceeding determines the patentability of claims in an issued patent and, therefore, affects the rights of the public. Under 35 U.S.C. § 316(a)(1) and 37 C.F.R. § 42.14, the default rule is that all papers filed in an *inter partes* review are open and available for access by the public; a party, however, may file a motion to seal and the information at issue is sealed pending the outcome of the motion. It is, however, only "confidential information" that is protected from disclosure. 35 U.S.C. § 316(a)(7). In that regard, the Trial Practice Guide, 77 Fed. Reg. at 48,760, provides:

[8] Apple's exhibit list (Paper 65), filed with its Motion for Observation, also was filed under seal.

> The rules aim to strike a balance between the public's interest in maintaining a complete and understandable file history and the parties' interest in protecting truly sensitive information.
>
> . . .
>
> *Confidential Information*: The rules identify confidential information in a manner consistent with Federal Rule of Civil Procedure 26(c)(1)(G), which provides for protective orders for trade secret or other confidential research, development, or commercial information. § 42.54.

The standard for granting a motion to seal is "for good cause." 37 C.F.R. § 42.54(a). Achates, as movant, bears the burden of proof in showing entitlement to the requested relief. 37 C.F.R. § 42.20(c). Achates must explain why the information sought to be sealed constitutes "confidential information."

Achates has not met its burden to show that the emails, and the papers citing the emails, contain "confidential information." The emails contain discussions between Achates's two declarants, Mr. Radbel and Dr. Wang, regarding their opinions on the prior art at issue in this proceeding. *See* Exs. 1067, 1068. They do not appear to contain any trade secrets, research information, or information that would be commercially sensitive.

Achates makes three arguments in its Motion to Seal. First, Achates argues that the parties agreed not to permit discovery regarding the "process" of producing declarations and, therefore, had a "shared expectation that such information would be maintained confidentially and certainly not be made available to the public." Mot. to Seal 2-3. We addressed this issue in ruling on Apple's motion for additional discovery, and were not persuaded by Achates's argument regarding an alleged agreement between the parties. *See* Paper 58 at 8. For the same reasons, we

are not persuaded that the emails should be sealed as "confidential information" based on the alleged agreement.

Second, Achates argues that the emails contain "confidential communications with and at the direction of counsel," and are "immune from discovery at least under the doctrine of work-product immunity." Mot. to Seal 3 & n.1. Similar to the argument it made in connection with Apple's motion for additional discovery, Achates does not cite any case law or explain in any detail *why* it believes the emails are privileged. *See* Paper 58 at 8. Moreover, Achates did not seek rehearing of our decision granting the motion for additional discovery, and produced the emails to Apple. We also note that, contrary to Achates's assertion that the emails are confidential communications "with" counsel, the emails at issue are "directly" between Mr. Radbel and Dr. Wang, in accordance with the limited additional discovery we authorized. *See id*. at 9; Exs. 1067, 1068.

Third, Achates contends that because Apple's observations are "rank speculation and offer no insights into the credibility" of Mr. Radbel and Dr. Wang, the Board should not review them in its analysis and "there is no need to make [the emails] available to the public." Mot. to Seal 3-4. Whether an opposing party's position regarding a document ultimately has merit, however, is not the test for determining whether the document should be sealed. The test is whether the material contains "confidential information," and Achates has not shown that the emails do.

As Achates provides no basis for deeming the emails to contain "confidential information," its Motion to Seal is denied. Papers 64, 65, and 69, and Exhibits 1067 and 1068, will be unsealed, and access to the

materials in the Patent Review Processing System (PRPS) will be changed from "Parties and Board Only" to "Public."

I. Achates's Motion to Exclude

In its Motion to Exclude, Achates seeks to exclude the declaration of Mr. Schneier (Exhibit 1003) submitted by Apple with the Petition. For the reasons discussed below, the motion is denied.

With few exceptions, the Federal Rules of Evidence apply to *inter partes* review proceedings. 37 C.F.R. § 42.62(a). The rules governing *inter partes* review set forth the proper procedure for objecting to, and moving to exclude, evidence when appropriate. When a party objects to evidence that was submitted during a preliminary proceeding, such an objection must be served within ten business days of the institution of trial. 37 C.F.R. § 42.64(b)(1). The objection to the evidence must identify the grounds for the objection with sufficient particularity to allow correction in the form of supplemental evidence. *Id*. This process allows the party relying on the evidence to which an objection is served timely the opportunity to correct, by serving supplemental evidence within ten business days of the service of the objection. *See* 37 C.F.R. §§ 42.64(b)(1), 42.64(b)(2). If, upon receiving the supplemental evidence, the opposing party is still of the opinion that the evidence is inadmissible, the opposing party may file a motion to exclude such evidence. 37 C.F.R. § 42.64(c).

Achates alleges various reasons why Mr. Schneier's declaration (Exhibit 1003) should be excluded. Mot. to Exclude 1-8. The declaration, however, was submitted by Apple with its Petition for *inter partes* review (Paper 1). Because the evidence was submitted during a preliminary

proceeding, any objection to such evidence must have been served within ten business days of the institution of the trial. 37 C.F.R. § 42.64(b)(1). Achates does not allege that Apple was served with any objection within ten business days of the institution of trial (Paper 21, dated June 3, 2013) or at any other time. Instead, Achates submits that 37 C.F.R. § 42.64 does not apply "because the bases of the objections arose when [Apple] failed to update Mr. Schneier's declaration as part of its Reply." Mot. to Exclude 7. Achates does not point to any rule or authority in support of the theory that Apple had a duty to "update" a declaration that was submitted with the Petition for *inter partes* review. Moreover, Apple would have had the right to serve supplemental evidence for the purpose of correcting any evidentiary deficiencies in the declaration, had Apple been provided with proper and timely notice, as required by 37 C.F.R. § 42.64. Thus, we are not persuaded that Mr. Schneier's declaration should be excluded.

III. ORDER

Apple has demonstrated, by a preponderance of the evidence, that:

(1) claims 1-3 are anticipated by Ginter under 35 U.S.C. § 102(e);

(2) claims 1-4 are unpatentable over Pettitt and Beetcher under 35 U.S.C. § 103(a); and

(3) claims 1-4 are unpatentable over Beetcher and Ginter under 35 U.S.C. § 103(a).

In consideration of the foregoing, it is hereby:

ORDERED that claims 1-4 of the '889 patent have been shown to be unpatentable;

FURTHER ORDERED that Achates's Motion to Exclude is *denied*;

FURTHER ORDERED that Achates's Motion to Seal is *denied*;

FURTHER ORDERED that Papers 64, 65, and 69, and Exhibits 1067 and 1068, are unsealed; and

FURTHER ORDERED that the copies of Exhibits 1003 and 1041 filed on December 14, 2012, are expunged from the record of this proceeding.

This is a final decision. Parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

Case IPR2013-00081
Patent 5,982,889

PETITIONER:

Jeffrey P. Kushan
Joseph A. Micallef
SIDLEY AUSTIN LLP
jkushan@sidley.com
jmicallef@sidley.com

PATENT OWNER:

Brad D. Pedersen
Eric H. Chadwick
PATTERSON THUENTE PEDERSEN, P.A.
prps@ptslaw.com
chadwick@ptslaw.com

Jason Paul DeMont
KAPLAN BREYER SCHWARTZ & OTTESEN
jpdemont@kbsolaw.com

Vincent McGeary
GIBBONS, P.C.
vmcgeary@gibbonslaw.com

US005982889A

United States Patent [19]

DeMont

[11] Patent Number: 5,982,889

[45] Date of Patent: Nov. 9, 1999

[54] **METHOD AND APPARATUS FOR DISTRIBUTING INFORMATION PRODUCTS**

[76] Inventor: **Jason Paul DeMont**, 244 English Place, Basking Ridge, N.J. 07920

[21] Appl. No.: **08/845,805**

[22] Filed: **Apr. 30, 1997**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/4**; 380/23; 280/286.4

[58] **Field of Search** 380/3, 4, 9, 21, 380/23, 44, 45, 49, 59; 711/152; 395/218, 186, 187.01, 188.01, 602, 609, 610, 612, 712, 762, 726, 728, 729, 730, 384–389; 340/825.31, 823.34; 341/78–82; 364/400, 479.04, 479.07; 270/222.81, 222.82, 222.9, 222.5–222.7; 260/265.2, 265.3; 280/286.4

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,683,968	8/1987	Applebaum et al.	380/4
4,845,715	7/1989	Francisco	371/53
5,103,476	4/1992	Waite et al	380/4
5,222,134	6/1993	Waite	380/4
5,337,357	8/1994	Chou et al.	380/4
5,343,526	8/1994	Lassers	380/4
5,490,216	2/1996	Richardson	380/4
5,553,139	9/1996	Ross et al.	380/4
5,579,222	11/1996	Bains et al.	395/712
5,625,690	4/1997	Michel et al.	380/4
5,636,277	6/1997	Nagahama	380/4
5,666,411	9/1997	McCarty	380/4
5,751,805	5/1998	Otsuki et al.	380/4
5,758,069	5/1998	Olsen	395/187.01

Primary Examiner—Tod R. Swann
Assistant Examiner—Paul E. Callahan

[57] **ABSTRACT**

A method and apparatus for distributing information products is described that includes the steps of generating a string, R; encrypting a first authentication code, an indicium of an end-user's identity, an indicium of a first information product, and an indicium of a second information product with the string, R, as the key to create a launch code; decrypting the launch code with the string, R, to recover the authentication code, the indicium of the end-user's identity, the indicium of the first information product and the indicium of the second information product; and installing the first information product and the second information product onto a computer associated with the end-user.

4 Claims, 4 Drawing Sheets

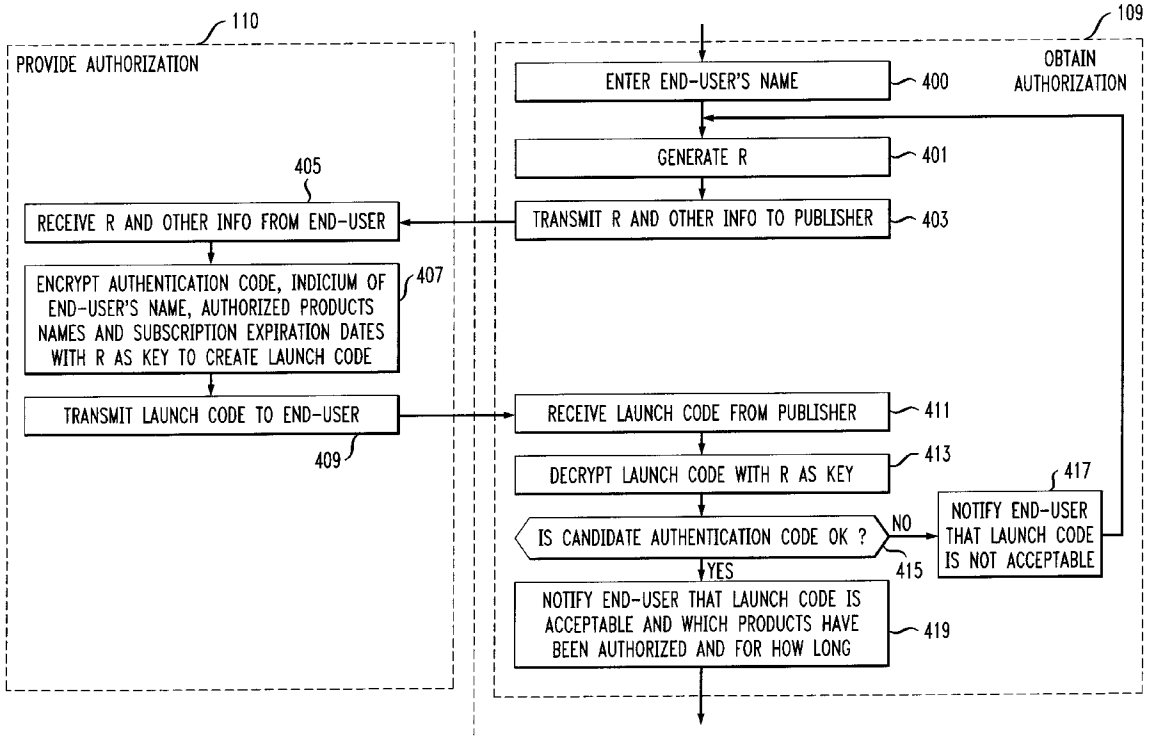


FIG. 1

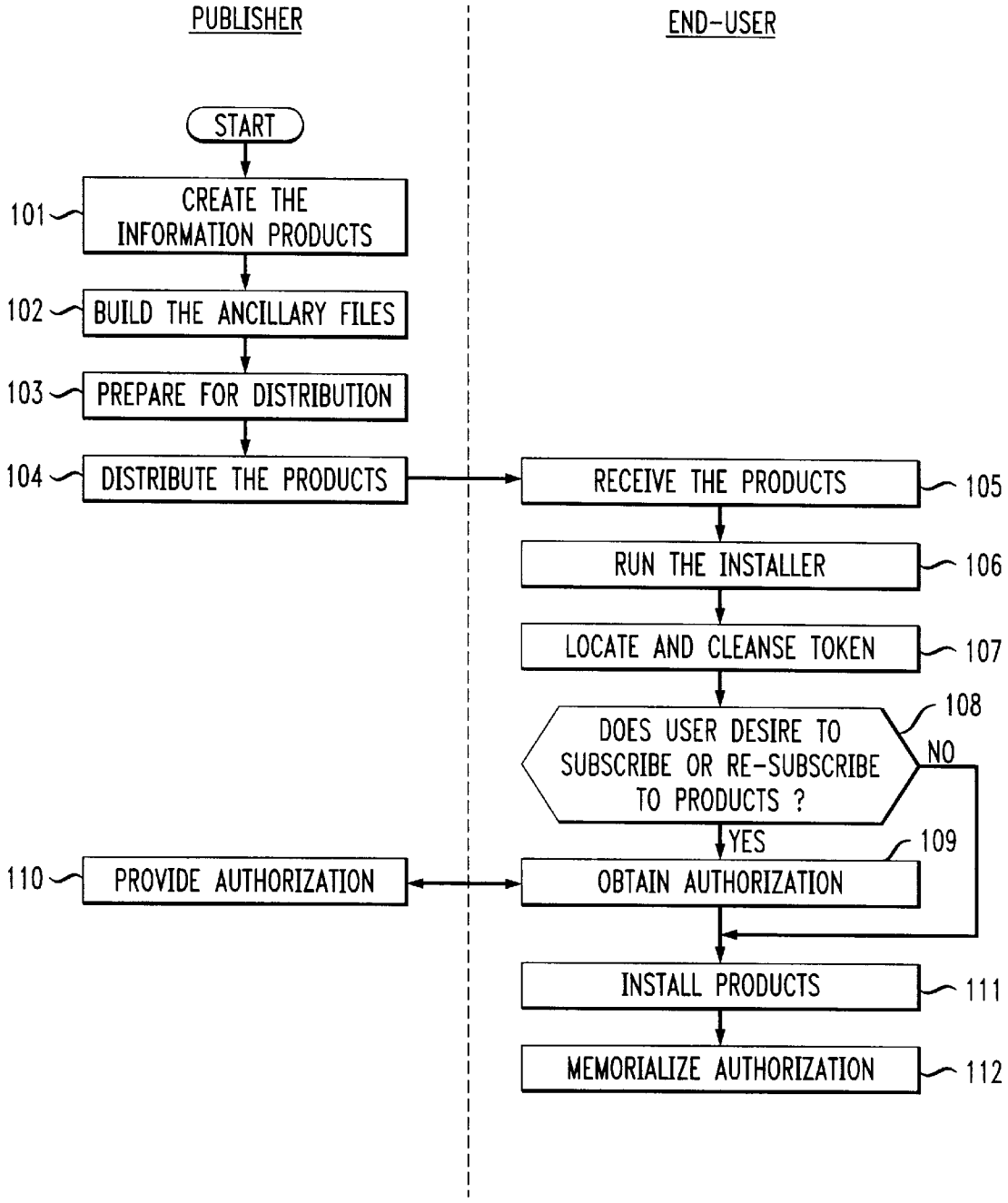

PUBLISHER
END-USER
START
101
CREATE THE INFORMATION PRODUCTS
102
BUILD THE ANCILLARY FILES
103
PREPARE FOR DISTRIBUTION
104
DISTRIBUTE THE PRODUCTS
RECEIVE THE PRODUCTS
105
RUN THE INSTALLER
106
LOCATE AND CLEANSE TOKEN
107
DOES USER DESIRE TO SUBSCRIBE OR RE-SUBSCRIBE TO PRODUCTS ?
108
NO
YES
109
110
PROVIDE AUTHORIZATION
OBTAIN AUTHORIZATION
INSTALL PRODUCTS
111
MEMORIALIZE AUTHORIZATION
112

FIG. 2

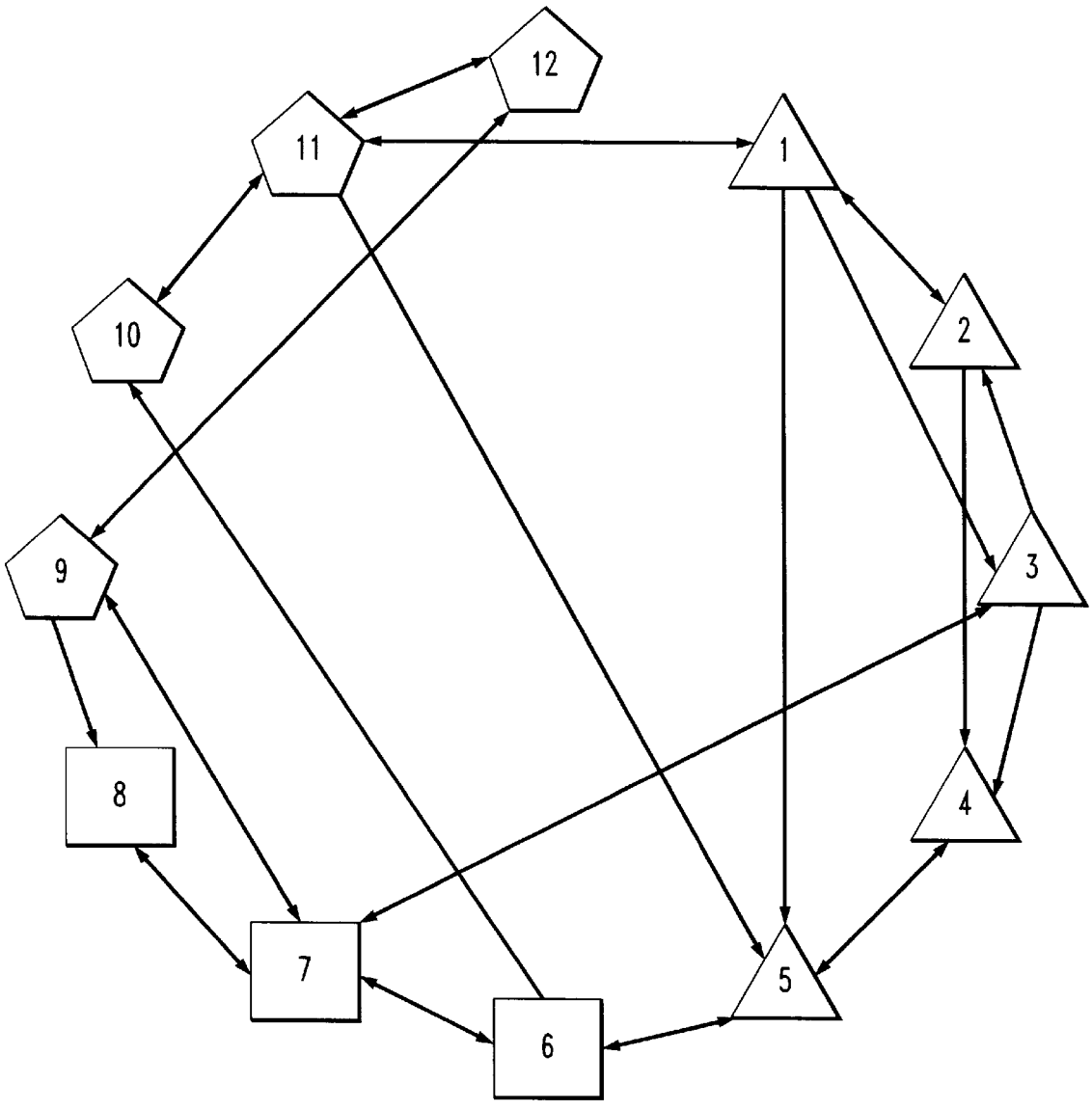
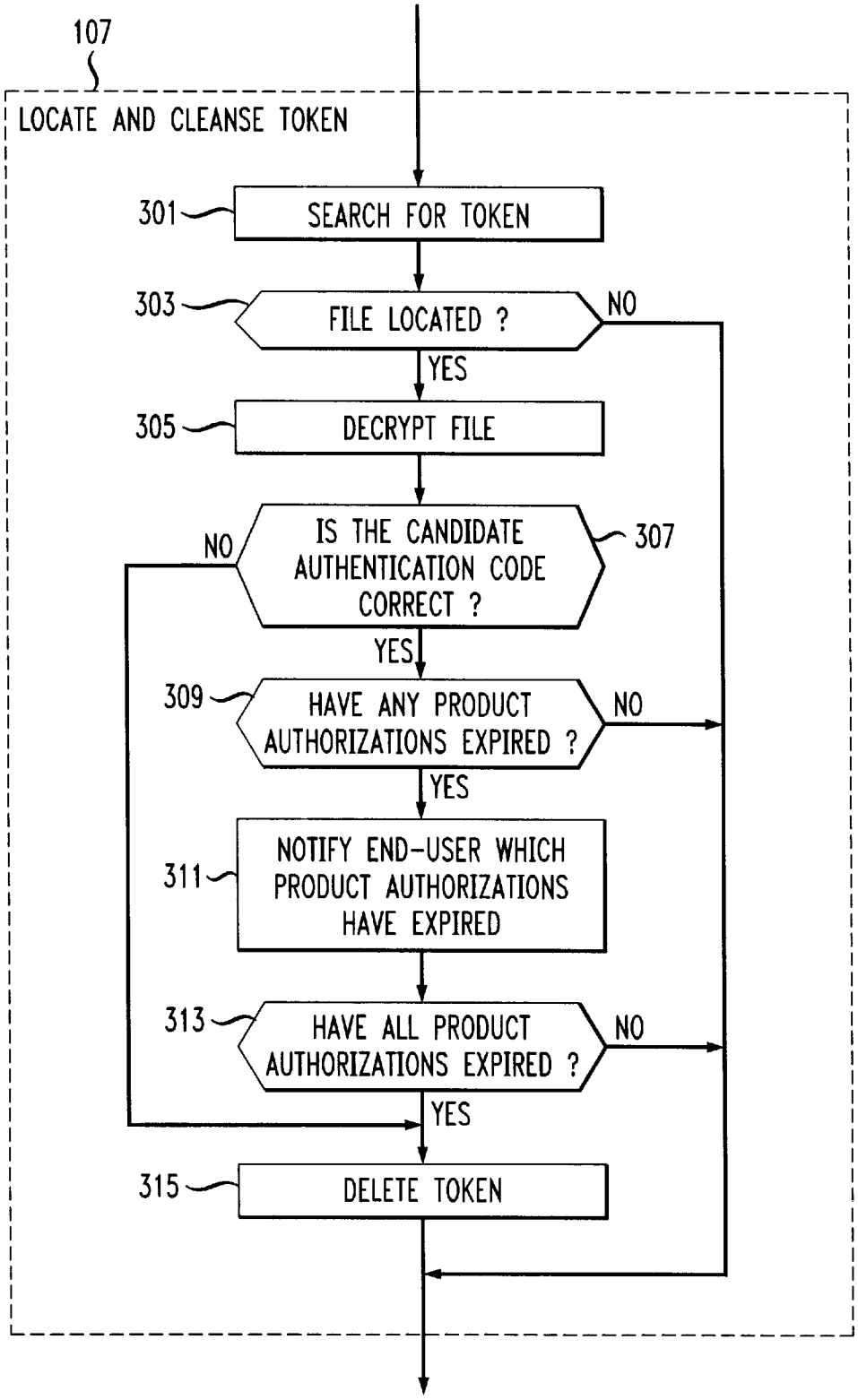


FIG. 3


107
LOCATE AND CLEANSE TOKEN
301
SEARCH FOR TOKEN
303
FILE LOCATED ?
NO
YES
305
DECRYPT FILE
NO
IS THE CANDIDATE AUTHENTICATION CODE CORRECT ?
307
YES
309
HAVE ANY PRODUCT AUTHORIZATIONS EXPIRED ?
NO
YES
311
NOTIFY END-USER WHICH PRODUCT AUTHORIZATIONS HAVE EXPIRED
313
HAVE ALL PRODUCT AUTHORIZATIONS EXPIRED ?
NO
YES
315
DELETE TOKEN

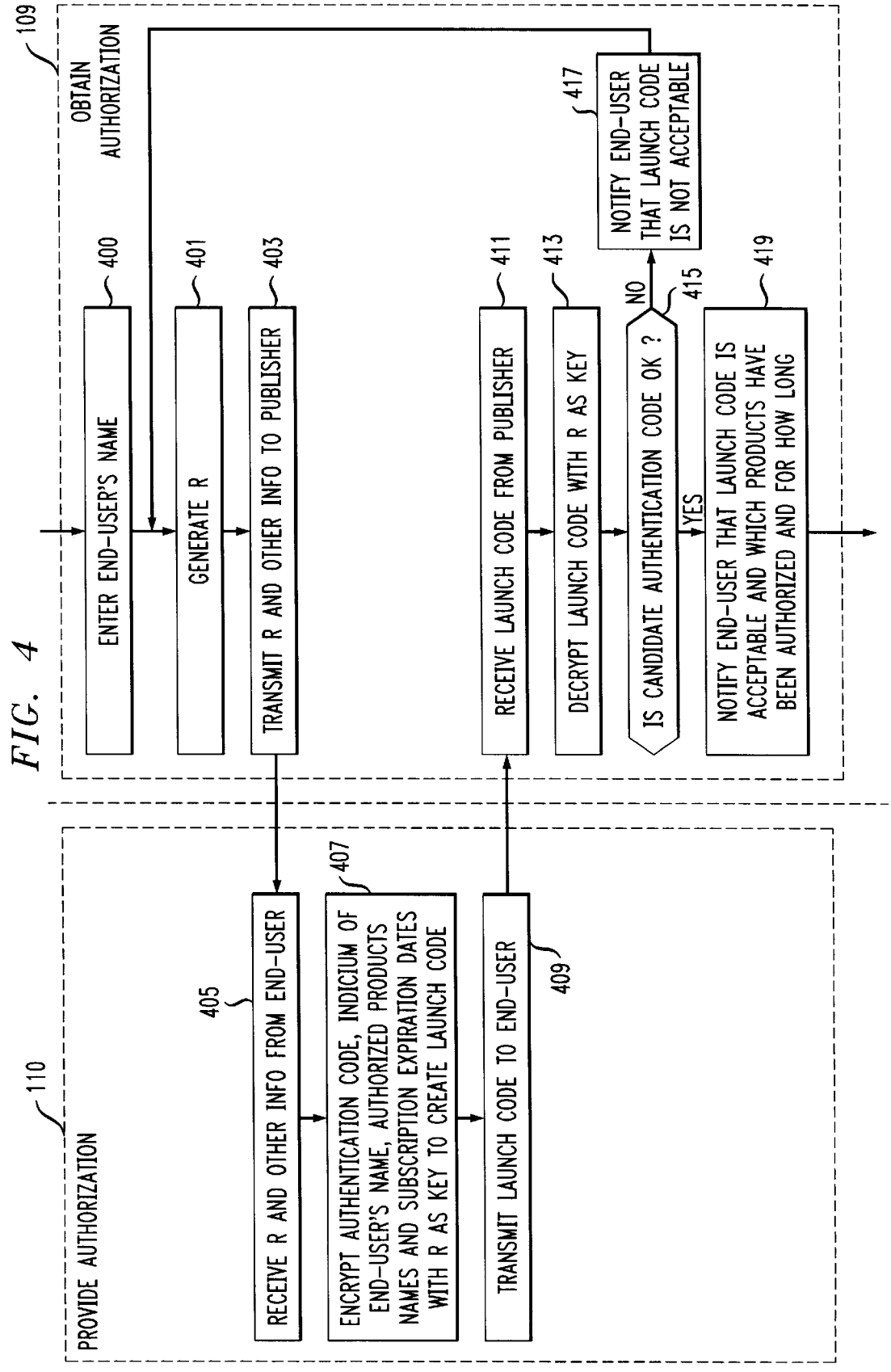

109
OBTAIN AUTHORIZATION
400
ENTER END-USER'S NAME
401
GENERATE R
403
TRANSMIT R AND OTHER INFO TO PUBLISHER
411
RECEIVE LAUNCH CODE FROM PUBLISHER
413
DECRYPT LAUNCH CODE WITH R AS KEY
415
IS CANDIDATE AUTHENTICATION CODE OK ?
NO
417
NOTIFY END-USER THAT LAUNCH CODE IS NOT ACCEPTABLE
YES
419
NOTIFY END-USER THAT LAUNCH CODE IS ACCEPTABLE AND WHICH PRODUCTS HAVE BEEN AUTHORIZED AND FOR HOW LONG
110
PROVIDE AUTHORIZATION
405
RECEIVE R AND OTHER INFO FROM END-USER
407
ENCRYPT AUTHENTICATION CODE, INDICIUM OF END-USER'S NAME, AUTHORIZED PRODUCTS NAMES AND SUBSCRIPTION EXPIRATION DATES WITH R AS KEY TO CREATE LAUNCH CODE
409
TRANSMIT LAUNCH CODE TO END-USER

FIG. 4

METHOD AND APPARATUS FOR DISTRIBUTING INFORMATION PRODUCTS

FIELD OF THE INVENTION

The present invention relates to a method and apparatus for distributing information products in general, and, more particularly, to a method and apparatus for distributing and installing computer programs and data.

BACKGROUND OF THE INVENTION

For as long as publishers have been distributing information products, piracy has been a concern. For the purposes of this specification the term "information product" includes, but is not limited to computer software, data, images, music, applets, photographs, animations, video, audio, text, hypertext and multimedia works.

As a practical matter, large-scale piracy committed by professional thieves is easier for publishers to detect and police because of the inherently commercial and public aspects of large-scale piracy. Small-scale piracy committed by individuals who, for example, purchase one copy of a computer program and install it on three or four computers in a small office are more insidious and, in the aggregate, economically more harmful to publishers.

Several techniques have been used by publishers of information products to impede piracy. When music was first distributed on CDs, CD duplicating equipment were expensive and rare and publishers implicitly relied on "physical security" to impede small-scale copyright infringers. The theory underlying physical security is that the difficulty in duplicating the media containing the information product is sufficient to stop most small-scale infringement.

When it is difficult for the end-user to duplicate the media, or to transfer the information product from one computer to another over a network, the publisher can be reasonably assured that widespread piracy is not occurring. Of course, the end-user could lend, lease or sell the media embodying the information product to another who would install it, and physical security could not prevent it.

When the technology for duplicating the media embodying an information product becomes ubiquitous, or it becomes easy to copy the information product from one computer to another over a network, publishers often employ "cryptographic security" to thwart copyright infringers.

According to one technique, the installer accompanying the software will not install the software on the end-user's computer until an acceptable password is entered by the end-user at the time of installation. The password is received by the end-user from the publisher after the end-user registers with the publisher and the publisher is assured that the end-user has paid for the software. Although this technique is widely used, it suffers from the weakness that the end-user can use the media and password again to install the software on another computer. Furthermore, the end-user can post the password publicly on an electronic bulletin-board and the advantage of the secret password are lost.

SUMMARY OF THE INVENTION

Some embodiments of the present invention are capable of distributing information products without many of the costs and restrictions associated with techniques in the prior art. In particular, some embodiments of the present invention are capable of distributing one or more information products together (e.g., either on a single CD-ROM or electronically over a network) while reserving to the publisher the ability to control which products are actually installed on an end-user's computer.

An illustrative embodiment of the present invention comprises the steps of: generating a string, R; encrypting a first authentication code, an indicium of an end-user's identity, an indicium of a first information product, and an indicium of a second information product with said string, R, as the key to create a launch code; decrypting said launch code with said string, R, to recover said authentication code, said indicium of said end-user's identity, said indicium of said first information product and said indicium of said second information product; and installing said first information product and said second information product onto a computer associated with said end-user.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** depicts a flowchart of the steps associated with distributing information products in accordance with the illustrative embodiment of the present invention.

FIG. **2** depicts a directed graph that indicates which files in a group of files contain hypertext links to which other files.

FIG. **3** depicts a flowchart of the detailed steps associated with the step of locating and cleansing the token in FIG. **1**.

FIG. **4** depicts a flowchart of the detailed steps associated with the steps of providing authorization and obtaining information in FIG. **1**.

DETAILED DESCRIPTION

The illustrative embodiment of the present invention facilitates the distribution of a plurality of information products by a publisher in such a manner that each product can be licensed, installed and used independently or in combination with other information products. Advantageously, this is accomplished, in part, through the use of a program commonly known as an "installer." As is well known to those skilled in the art, an installer is program that is prepared by the publisher of an information product, that is distributed along with the information product, and that controls the installation of the information product onto the end-user's computer. Although the installer runs on the end-user's computer, it acts as remote agent of the publisher to control how and under what circumstances the information products are installed on the end-user's computer.

Each information product associated with the illustrative embodiment constitutes a plurality of hypertext files or "web pages" that are accessed by the end-user through a browser such as Netscape Navigator or Internet Explorer. Although each information product comprises hypertext files, the files are not intended to be accessed by the end-user via the Internet. Instead, all of the information products are advantageously distributed together on a single medium (e.g., a CD-ROM) or electronically (e.g., via the Internet) and are installed on the end-user's computer, or on an intranet server associated with the end-user. It will be clear to those skilled in the art how to use a browser such as Netscape Navigator or Internet Explorer to browse through web pages that are stored locally in contrast to using the browser to browse web pages that are stored on http servers across the Internet.

One example of an information product that can be used with embodiments of the present invention comprises a plurality of web pages that constitute some of the legislative, administrative and judicial materials associated with patent

law. Another example of an information product that can be used with embodiments of the present invention comprises a plurality of web pages that constitute some of the legislative, administrative and judicial materials associated with trademark law. And yet another example of an information product that can be used with embodiments of the present invention comprises a plurality of web pages that constitute some of the legislative, administrative and judicial materials associated with copyright law.

Information products that work with embodiments of the present invention need not relate to law, or reference materials, or even text. Other information products could comprise music, video, multimedia, or data or other executables. It will be clear to those skilled in the art how to make and use the embodiments of the invention that are associated with information products that comprise other than hypertext files.

Each information product associated with the illustrative embodiment constitutes a single issue of a periodical to which an end-user can subscribe and receive monthly updates. It will be clear to those skilled in the art that other embodiments of the present invention can be used to distribute a single information product. It will also be clear to those skilled in the art that other embodiments of the present invention can be used to distribute one or more information products that are not part of a serialization or that are part of a serialization that issues sporadically, in contrast to periodically.

FIG. **1** depicts a flowchart that outlines the steps associated with distributing information products in accordance with the illustrative embodiment of the present invention.

I. Create The Information Products

In accordance with step **101**, each information product is created by the publisher. To assist in describing the illustrative embodiment, three information products are created whose subject matter is related. For the purposes of this specification, the three products are named "Patent Law Library," "Trademark Law Library" and "Copyright Law Library." It will be clear to those skilled in the art how to make and use embodiments of the present invention when a different number of products are created, or when their subject matter is not related, or both.

For the purposes of the illustrative embodiment, the Patent Law Library is a set of files that contain Title 35 of the United States Code as marked-up in the Hypertext Markup Language ("HTML"); the Trademark Law Library is a set of files that contain the Lanham Act as marked-up in HTML, and the Copyright Law Library is a set of files that contain Title 17 of the United States Code as marked-up in HTML. The files in each information product are advantageously viewed on an end-user's computer through a browser such as Netscape Navigator or Internet Explorer.

Although all three products are advantageously distributed together, any one, two or all three of the products can be installed into an end-user's computer. In other words, in accordance with the illustrative embodiment, one end-user can install just the Patent Law Library although another installs both Patent Law Library and Copyright Law Library.

Because of the perishable nature of the subject matter of each of the illustrative products, the Patent Law Library, Trademark Law Library and Copyright Law Library are each a single issue of a periodical, which issues monthly.

Each product advantageously comprises one or more files within one or more directories in a hierarchical file structure. When a product contains a large number of files, it is usually advantageous to arrange the files in multiple directories. It will be clear to those skilled in the art how to determine when a specific information product should contain multiple directories. For pedagogical reasons, the files within each of the three illustrative information products are contained within a single directory.

Some or all of the files in the illustrative information products advantageously contain hypertext links to items in other files. For example, the reference in 35 U.S.C. 42(c) to section 31 of the Lanham Act can be implemented as a hypertext link from the file containing 35 U.S.C. 42(c) in the Patent Law Library to the file containing section 31 in the Trademark Law Library.

It will be clear to those skilled in the art that files associated with other embodiments of the present invention can contain, for example, executable programs, data and/or references to other files, which target files may be in the same or other products. It will also be clear to those skilled in the art that information products associated with other embodiments of the present invention need not contain references to other files. It will be clear to those skilled in the art how to create the files in each product.

All of the files in all of the products are advantageously created and arranged in a file structure with the knowledge of the name and location in the file structure of each file it is capable of referencing, regardless of whether the files are part of the same information product or not.

The Patent Law Library comprises five files in the hierarchical file structure shown in Table 1. The Trademark Law Library comprises three files in the hierarchical file structure shown in Table 2, and the Copyright Law Library comprises four files in the hierarchical file structure shown in Table 3. Advantageously, all three products are designed to install into the same hierarchical directory space, relative to whatever the end-user defines, during installation, as the root directory for the product(s).

TABLE 1

The files that compose the Patent Law Library.

File	Location
File 1	\directory1\file1.htm
File 2	\directory1\file2.htm
File 3	\directory1\file3.htm
File 4	\directory1\file4.htm
File 5	\directory1\file5.htm

TABLE 2

The files that compose the Trademark Law Library.

File	Location
File 6	\directory2\file6.htm
File 7	\directory2\file7.htm
File 8	\directory2\file8.htm

TABLE 3

The files that compose the Copyright Law Library.

File	Location
File 9	\directory3\file9.htm
File 10	\directory3\file10.htm
File 11	\directory3\file11.htm
File 12	\directory3\file12.htm

For pedagogical reasons, the three information products in the illustrative embodiment comprise a total of 12 files. In commercial applications, it will be clear to those skilled in the art that a single information product can comprise hundreds or thousands of files. It will be clear to those skilled in the art how to make and use the files that compose the three products.

The books *HTML Publishing for Netscape*, Stuart Harris & Gayle Kidder, Ventana Communications Group, Inc., Research Triangle Park, N.C., and *HTML: The Definitive Guide*, Chuck Musciano & Bill Kennedy, O'Reilly & Associates, Inc., Sebastopol, Calif., provide an excellent overview the creation of files using HTML and are incorporated by reference.

II. Build The Ancillary Files

Because (1) each file can contain a hypertext link to a target file that may not be in the same information product, and (2) the information products can be licensed and installed separately, the possibility exists that a file can be installed on a end-user's computer that contains a hypertext link to a target file that is not installed on the end-user's computer. The result is a hypertext link that, when executed, generates a run-time error because the target file is not installed on the computer.

To preclude run-time errors, the installer advantageously installs a "dummy" or "nominal" file into the end-user's computer in the same location and with the same name as each file that could be referenced but is not also installed. The nominal file advantageously does not contain the same information as the authentic file, but contains a notice that it is only a nominal file and that access to the authentic file requires the installation of another information product.

At step **102**, ancillary files are built to enable the installer to know where to install the nominal files. In the illustrative embodiment, one ancillary file is built for each information product and the ancillary files indicates the name and location of each nominal file to be installed when that information product is installed.

There are two alternative techniques that can be used by the installer for installing the nominal files and the authentic files. According to the first technique, the installer installs all of the authentic files for all of the information products to be installed, and then installs all of the nominal files into those locations not containing an authentic file. According to the second technique, the installer installs all of the nominal files for all of the information products to be installed, and then installs all of the authentic files to be installed over the nominal files, perhaps overwriting over some or all of the nominal files. The choice of technique advantageously does not affect how the ancillary files are built. The installer associated with the illustrative embodiment uses the first technique, but it will be clear to those skilled in the art how to make and use embodiments of the present invention that use the second technique.

When the total number of files in all of the information products is small, each ancillary file associated with each information product can exhaustively list all of the files associated with every other information product. In contrast, when the total number of files in all of the information products is large, it is advantageous for each ancillary file to list only those files actually needed. To determine which files are needed, all of the files in all of the information products need to be examined to determine which files reference which other files.

FIG. **2** depicts an illustrative directed graph that represents all of the files in the three illustrative products and indicates which files contain hypertext links to other files. It will be clear to those skilled in the art how to determine the topology of the directed graph by examining all of the files in all of the products associated with an embodiment of the present invention.

Each file in each product is represented by a polygon enclosing a number. Each of the five files associated with the Patent Law Library are depicted by a triangle; each of the three files associated with the Trademark Law Library are depicted by a square and each of the four files associated with the Copyright Law Library are depicted by a pentagon. The number inside the polygon indicates exactly which file it is associated with. For example, the file "file3.htm" is depicted by a triangle enclosing the number 3.

An arrow from one polygon to another indicates that the file associated with the first polygon contains at least one hypertext link to the file associated with the second polygon. A double-ended arrow indicates that both files contain hypertext links to each other.

Table 4 provides the same information as does FIG. **2**, but in tabular format. Each row in Table 4 represents a file in one of the three products, and an "X" in a box means that the file associated with the row contains a hypertext link to the file associated with that column. Like the directed graph in FIG. **2**, the entries in Table 4 are illustrative only. It will be clear to those skilled in the art how to make a similar table by examining all of the files in all of the information products associated with an embodiment of the present invention.

Although both the directed graph of FIG. **2** and Table 4 illustrate a tendency for files within an information product to reference other files within the same product, there are occurrence of files within one product containing references to files in other products.

TABLE 4

Which Files Externally Reference Which Files

	1	2	3	4	5	6	7	8	9	10	11	12
1		X	X		X						X	
2	X			X								
3		X		X			X					
4					X							
5				X		X						
6					X		X			X		
7			X			X		X	X			
8							X					
9							X	X				X
10											X	
11	X				X					X		X
12									X		X	

As both FIG. **2** and Table 4 indicate, there are three files (File **6**, File **7** and File **11**) not within the Patent Law Library that are referenced by files within Patent Law Library. Therefore, the Patent Law Library's ancillary file is built as shown in Table 5. Whenever the Patent Law Library is installed, the files listed in the ancillary file are advantageously also installed as nominal files.

TABLE 5

Ancillary File associated with the Patent Law Library

Ancillary File
\directory2\file6.htm
\directory2\file7.htm
\directory3\file11.htm

As both FIG. **2** and Table 4 indicate, there are four files (File **3**, File **5**, File **9** and File **10**) not within the Trademark Law Library that are referenced by files within Trademark Law Library. Therefore, the Trademark Law Library's ancillary file is built as shown in Table 6. Whenever the Trademark Law Library is installed, the files listed in the ancillary file are advantageously also installed as nominal files.

TABLE 6

Ancillary File associated with the Trademark Law Library

Ancillary File
\directory1\file3.htm
\directory1\file5.htm
\directory3\file9.htm
\directory3\file10.htm

As both FIG. **2** and Table 4 indicate, there are four files (File **1**, File **5**, File **7** and File **8**) not within the Copyright Law Library that are referenced by files within Copyright Law Library. Therefore, the Copyright Law Library's ancillary file is built as shown in Table 7. Whenever the Copyright Law Library is installed, the files listed in the ancillary file are advantageously also installed as nominal files.

TABLE 7

Ancillary File associated with the Copyright Law Library

Ancillary File
\directory1\file1.htm
\directory1\file5.htm
\directory2\file7.htm
\directory2\file8.htm

III. Prepare For Distribution

Referring again to step **103** in FIG. **1**, when each information product and its associated ancillary file are built, the files are advantageously prepared for distribution. Because all of the information products are advantageously distributed on the same medium (e.g., CD-ROM, DVD, diskette) or distributed electronically over a wide-area-network (e.g., the Internet), each information product is advantageously compressed with a lossless compression technique and encrypted, in well-known fashion, with the string, S, as the key.

The purpose of the compression is to reduce the amount of bandwidth each information product consumes during distribution and to reduce the entropy of the information products before encryption. The purpose of encryption is to enable the distribution of the information products without allowing unauthorized access to the information products after the information products have left the publisher's possession. In other words, the encryption allows the publisher to give a potential end-user a CD-ROM that contains all of information products but to retain control of the end-user's access to the information products. The installer is advantageously knows the cryptosystem and key for decrypting each of the information products. How the publisher grants access to the information products after they have left his or her control will be described in detail below.

It will be clear to those skilled in the art how to prepare the information products and ancillary files for distribution.

IV. Distribute the Information Products

At step **104**, the information products and ancillary files and the accompanying installer and its associated files are distributed on a single medium (e.g., a CD-ROM, DVD), on

multiple media (e.g., diskettes) and/or electronically over a network (e.g., the Internet). It will be clear to those skilled in the art how to distribute the information products.

V. Receive the Information Products

At step **105**, the information products and ancillary files and the accompanying installer and its associated files are received by the end-user.

VI. Run the Installer

At step **106**, the end-user initiates the installation process. When the information products are distributed on one or more media, the end-user inserts the media into his or her computer and runs the installer in well-known fashion. When the information products are distributed electronically over a network, the end-user collects the files on his or her computer and then runs the installer in well-known fashion.

VI. Locate and Cleanse the Token

At step **107**, the installer advantageously checks to determine if the publisher has previously granted authorization to install one or more of the information products on the end-user's computer. The installer determines if the publisher has previously granted authorization by searching for a token on the end-user's computer, which token would have been placed there by an earlier edition of the installer from the publisher.

When an end-user obtains a subscription to one or more of the information products, the installer memorializes the authorization during the length of the subscription. This is advantageous because it relieves the publisher and the end-user from having to obtain explicit authorization for each issue during the length of the subscription.

The token can be conceptualized as a secret, authenticated message from one installer to a subsequent installer that indicates to the subsequent installer that the end-user's computer is granted access to certain of the information products for a given duration. How the token is created and placed on the end-user's computer will be described in detail below.

Advantageously, the token is a file with a name and location that are known to the installer. The token advantageously comprises a data structure comprising:

(1) an authentication code;

(2) an indication of the name of the end-user;

(3) a list of the information products to which the end-user has been granted access; and

(4) an indication of when the authorization for each information product expires.

Furthermore, the token file is encrypted so as to impede an end-user from illicitly obtaining access to an information product by doctoring the token. The encryption is performed, in well-known fashion, and the installer advantageously knows the both the cryptosystem and the key, T, for decrypting the token. Table 8 depicts the contents of the illustrative token.

TABLE 8

Contents of the Illustrative Token
Authentication code
Indication of End-User's Identity
Information Product No. 1; Expiration Date
Information Product No. 2; Expiration Date
...

The authentication code is advantageously a 32-bit or longer string that is known to the installer and publisher and is not generally known to the public.

The indication of the name of the user can either be the actual name of the end-user or a code that represents the name of the end-user. When a user illicitly attempts to share the token with others or to post it on a bulletin board or the Internet, it indelibly bears an indicium of the name of the person to whom it was originally given. If the publisher sees the token posted publicly, the publisher can decrypt the token, learn the identity of the user to whom the token was given and then investigate whether that users is inducing copyright infringement of the publisher's information products.

The list of information products to which the end-user has been authorized access can either list the products to which access has been authorized, or, alternatively, can list of all of the information products published and an indication of whether access has been authorized or not for each product.

The indication of when the access for each information product expires is advantageously based on the information products' version numbers rather than on calendar dates. Each edition of the installer is told what is the version number of the information products that accompany it.

FIG. **3** depicts a flowchart of the illustrative steps conducted by the installer in locating and cleansing the token, which is step **107** in FIG. **1**. At step **301**, the installer searches the end-user's computer for a file with the same name as the token and in the same location as expected. At step **303**, if the installer locates a file with the same name as the token and in the same location as expected, then control passes to step **305**, else the installer infers that authorization was not previously given. At step **305**, the installer decrypts the found file, in well-known fashion, according to the cryptosystem and the key it knows. At step **307**, the installer attempts to locate the candidate authentication code in the decrypted file and compares the candidate authentication code with the known authentication code, which the installer knows. If the installer determines that the candidate authentication code matches the known authentication code, the installer infers that the token is genuine and has not been doctored and control passes to step **309**; else the installer infers than authorization was not previously given or the token was doctored and control passes to step **315**. As a practical matter, a mismatched authentication code is likely to be the result of an end-user trying to gain unauthorized access to the information products by tinkering with the token.

At step **309**, the installer determines if the any of the information products' authorizations have expired. If the any of the information products' authorizations have expired, then control passes to step **311**. At step **311**, the installer notifies the end-user which information products' authorizations have expired, and then control passes to step **313**. At step **313**, the installer determines if all of the information products' authorizations have expired, and if they have, control passes to step **315**. At step **315**, the installer deletes the token.

VII. Subscribe or Re-Subscribe?

Referring to step **108** in FIG. **1**, the end-user is queried by the installer whether the end-user desires to subscribe to new information products or to re-subscribe to information products whose subscriptions have expired. If the end-user indicates "No," then control passes to step **111**. Otherwise, control passes to step **109**.

VIII. Obtain Authorization

At step **109** the end-user seeks authorization to subscription or re-subscribe to one or more information products. Because the various information products are encrypted, it is difficult for the end-user to access the information products

unilaterally and without the installer's cooperation. The end-user acquires the installers cooperation to decrypt and install the respective information products by entering into the installer a "password" or "launch code," which is chosen from a large number of possibilities so that probabilistically it is unlikely that the end-user can guess it. Advantageously, the publisher only provides the launch code to the end-user after the publisher is satisfied that the end-user has paid for access to the products.

FIG. **4** depicts a flowchart of the steps involved in the illustrative embodiment for obtaining and providing authorization to begin a subscription. First, at step **400** the installer advantageously requires that the end-user enter all or a portion of his or her name. At step **401**, the installer then generates and notifies the end-user of a 32-bit or longer "serial number," R, that is advantageously based on a random number generated by the installer. The serial number can also be based, in part, on the end-user's name, as input at step **400**. It is advantageous that the end-user not be able to control what serial number is generated, nor that the same serial number be generated each time step **401** is encountered.

At step **403**, the end-user then advantageously contacts the publisher via the telephone or the Internet and provides to the publisher:

(1) the end-user's name and address;

(2) the end-user's credit card information or other method of payment;

(3) the information products that the end-user desires to subscribe to and for what duration; and

(4) the serial number, R, generated by the installer at step **401**.

When the publisher is satisfied that he or she will be paid for the subscription, the publisher creates the launch code by encrypting a data structure comprising:

(1) a authentication code;

(2) an indication of the name of the end-user;

(3) a list of the information products to which the end-user has been granted access; and

(4) an indication of when the authorization for each information product expires

in a cryptosystem known to the installer using R as the key. Advantageously, only the publisher and the installer know the cryptosystem used for encrypting and decrypting the launch code. It will be clear to those skilled in the art how to create the launch code. At steps **409** and **411**, the publisher transmits the launch code to the end-user, who enters the launch code into the installer.

At step **413**, the installer decrypts the launch code with R as the key. At step **415**, the installer recovers the candidate authentication code from the decrypted launch code and determines if the candidate authentication code matches the authentication code known to the installer. When the authentication code matches, the installer infers that the launch code is authentic and control passes to step **419**. When the authentication code does not match, the installer infers that the launch code has been corrupted or doctored, and control passes to step **417**. At step **417** is end-user is notified by the installer that the launch code not accepted and control passes to step **401**.

At step **419**, the installer notifies the end-user that the launch code is accepted and also advantageously notifies the end-user that subscriptions for what product have been authorized and for what duration.

The purpose of generating a new serial number, R, each time the installer requires a launch code is to prevent the end-user from using a single launch code to install the information products on multiple computers. The purpose of encrypting the data structure at step **407** is to impede an end-user from manipulating the parameters in the data structure to get more than was paid for.

The purpose of putting an indication of the end-user's identity into the launch code is identical to the reason the indication of the end-user's identity was put into the token. That is, if an end-user shares the launch code with others or to post it on a bulletin board or the Internet, it indelibly bears the name of the person to whom it was originally given. If the publisher sees the launch code posted publicly, the publisher can decrypt the launch code, learn the identity of the user to whom the launch code was given and then investigate whether that end-user is inducing copyright infringement of the publisher's information products. Because the publisher may not know what value of R was used to encrypt that particular launch code, the existence of the known authentication code in the plaintext provides the publisher with information to make a known-plaintext cryptanalytic attack on the launch code.

IX. Install the Products

At step **111** in FIG. **1**, the installer installs all of the information products that have been authorized by the publisher to be installed. This includes both the information products whose authorization was given previously in the token, and the information products whose authorization was obtained in step **109**.

Advantageously, the installer decrypts the authorized information products and installs them on the end-user's computer in well-known fashion. Then the installer uses the ancillary file associated with each installed information product to install the nominal files, if any, on the end-user's computer, as described above.

X. Memorialize the Authentication

At step **112** in FIG. **1**, the installer memorializes the authorization of the various information products by updating the token located in step **107**, if necessary, with the new authorizations, if any, obtained in step **109**. The revised token is then advantageously encrypted with a cryptosystem and a key, T, that will be known to later editions of the installer. The encrypted token is then stored on the end-user's computer with a name and in location to be known by later editions of the installer.

What is claimed is:

1. A method comprising the steps of:

generating a string, R;

encrypting a first authentication code, an indicium of an end-user's identity, an indicium of a first information product, and an indicium of a second information product with said string, R, as the key to create a launch code;

decrypting said launch code with said string, R, to recover said authentication code, said indicium of said end-user's identity, said indicium of said first information product and said indicium of said second information product; and

installing said first information product and said second information product onto a computer associated with said end-user.

2. The method of claim **1** further comprising the steps of:

creating a token comprising a second authentication code, said indicium of said end-user's identity, said indicium of said first information product and said indicium of said second information product;

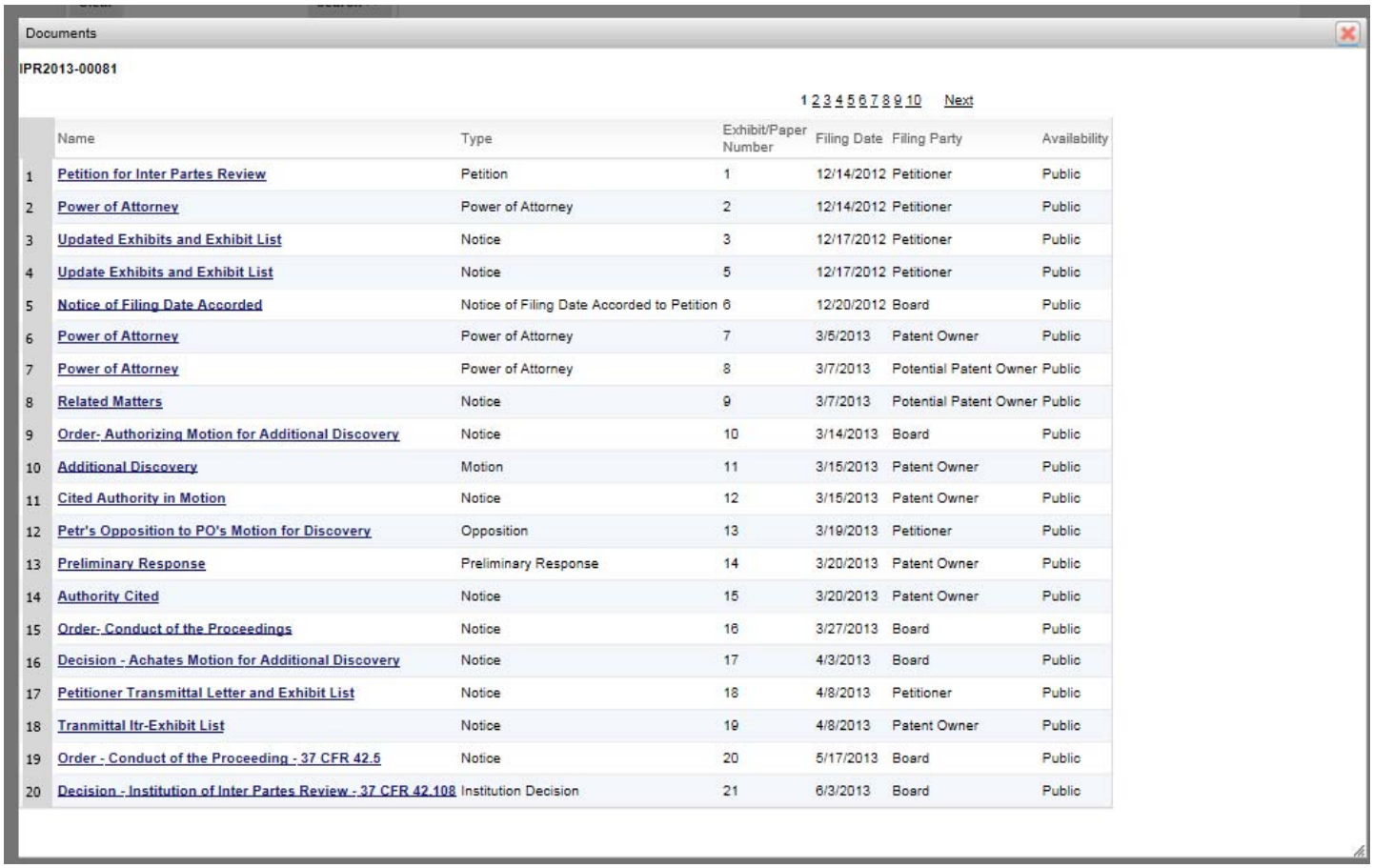
encrypting said token with a string, T, to create an encrypted token; and

storing said encrypted token on said computer.

3. The method of claim **2** wherein said first authentication code and said second authentication code are the identical.

4. The method of claim **2** wherein said string, R, and said string, T, are identical.

* * * * *

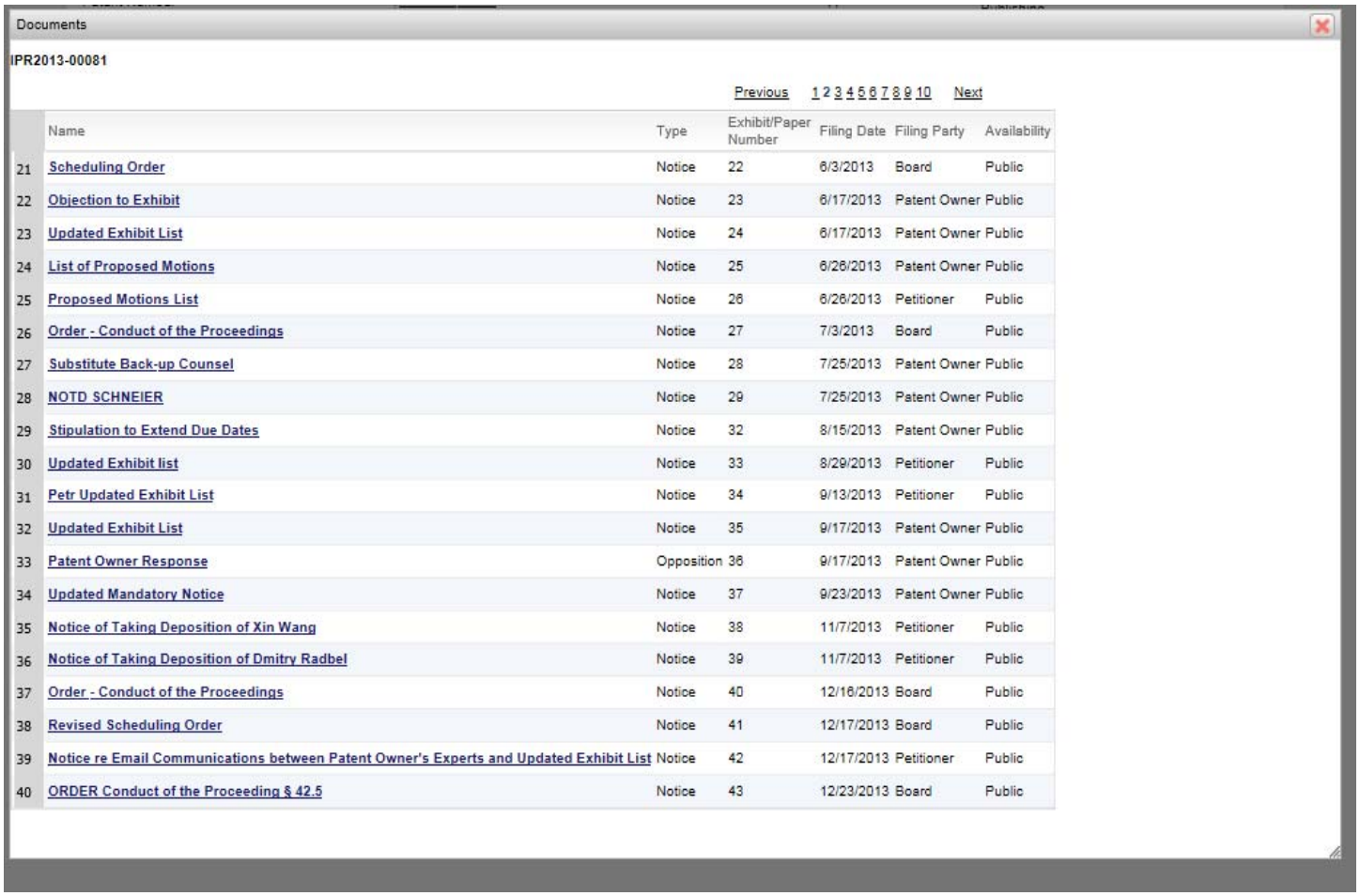


Documents

IPR2013-00081

1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
1	Petition for Inter Partes Review	Petition	1	12/14/2012	Petitioner	Public
2	Power of Attorney	Power of Attorney	2	12/14/2012	Petitioner	Public
3	Updated Exhibits and Exhibit List	Notice	3	12/17/2012	Petitioner	Public
4	Update Exhibits and Exhibit List	Notice	5	12/17/2012	Petitioner	Public
5	Notice of Filing Date Accorded	Notice of Filing Date Accorded to Petition	6	12/20/2012	Board	Public
6	Power of Attorney	Power of Attorney	7	3/5/2013	Patent Owner	Public
7	Power of Attorney	Power of Attorney	8	3/7/2013	Potential Patent Owner	Public
8	Related Matters	Notice	9	3/7/2013	Potential Patent Owner	Public
9	Order- Authorizing Motion for Additional Discovery	Notice	10	3/14/2013	Board	Public
10	Additional Discovery	Motion	11	3/15/2013	Patent Owner	Public
11	Cited Authority in Motion	Notice	12	3/15/2013	Patent Owner	Public
12	Petr's Opposition to PO's Motion for Discovery	Opposition	13	3/19/2013	Petitioner	Public
13	Preliminary Response	Preliminary Response	14	3/20/2013	Patent Owner	Public
14	Authority Cited	Notice	15	3/20/2013	Patent Owner	Public
15	Order- Conduct of the Proceedings	Notice	16	3/27/2013	Board	Public
16	Decision - Achates Motion for Additional Discovery	Notice	17	4/3/2013	Board	Public
17	Petitioner Transmittal Letter and Exhibit List	Notice	18	4/8/2013	Petitioner	Public
18	Tranmittal ltr-Exhibit List	Notice	19	4/8/2013	Patent Owner	Public
19	Order - Conduct of the Proceeding - 37 CFR 42.5	Notice	20	5/17/2013	Board	Public
20	Decision - Institution of Inter Partes Review - 37 CFR 42.108	Institution Decision	21	6/3/2013	Board	Public

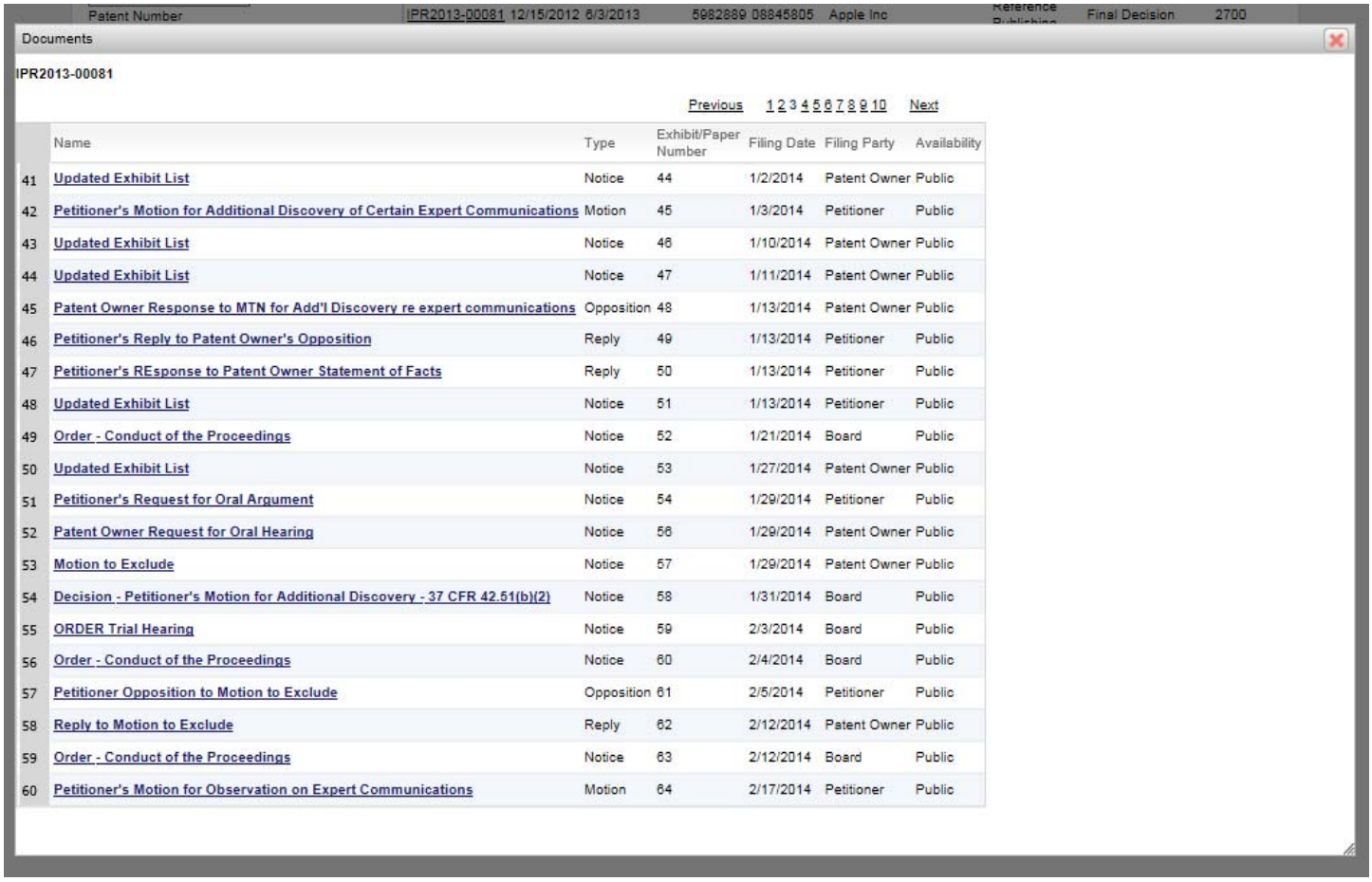


Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
21	Scheduling Order	Notice	22	6/3/2013	Board	Public
22	Objection to Exhibit	Notice	23	6/17/2013	Patent Owner	Public
23	Updated Exhibit List	Notice	24	6/17/2013	Patent Owner	Public
24	List of Proposed Motions	Notice	25	6/26/2013	Patent Owner	Public
25	Proposed Motions List	Notice	26	6/26/2013	Petitioner	Public
26	Order - Conduct of the Proceedings	Notice	27	7/3/2013	Board	Public
27	Substitute Back-up Counsel	Notice	28	7/25/2013	Patent Owner	Public
28	NOTD SCHNEIER	Notice	29	7/25/2013	Patent Owner	Public
29	Stipulation to Extend Due Dates	Notice	32	8/15/2013	Patent Owner	Public
30	Updated Exhibit list	Notice	33	8/29/2013	Petitioner	Public
31	Petr Updated Exhibit List	Notice	34	9/13/2013	Petitioner	Public
32	Updated Exhibit List	Notice	35	9/17/2013	Patent Owner	Public
33	Patent Owner Response	Opposition	36	9/17/2013	Patent Owner	Public
34	Updated Mandatory Notice	Notice	37	9/23/2013	Patent Owner	Public
35	Notice of Taking Deposition of Xin Wang	Notice	38	11/7/2013	Petitioner	Public
36	Notice of Taking Deposition of Dmitry Radbel	Notice	39	11/7/2013	Petitioner	Public
37	Order - Conduct of the Proceedings	Notice	40	12/16/2013	Board	Public
38	Revised Scheduling Order	Notice	41	12/17/2013	Board	Public
39	Notice re Email Communications between Patent Owner's Experts and Updated Exhibit List	Notice	42	12/17/2013	Petitioner	Public
40	ORDER Conduct of the Proceeding § 42.5	Notice	43	12/23/2013	Board	Public



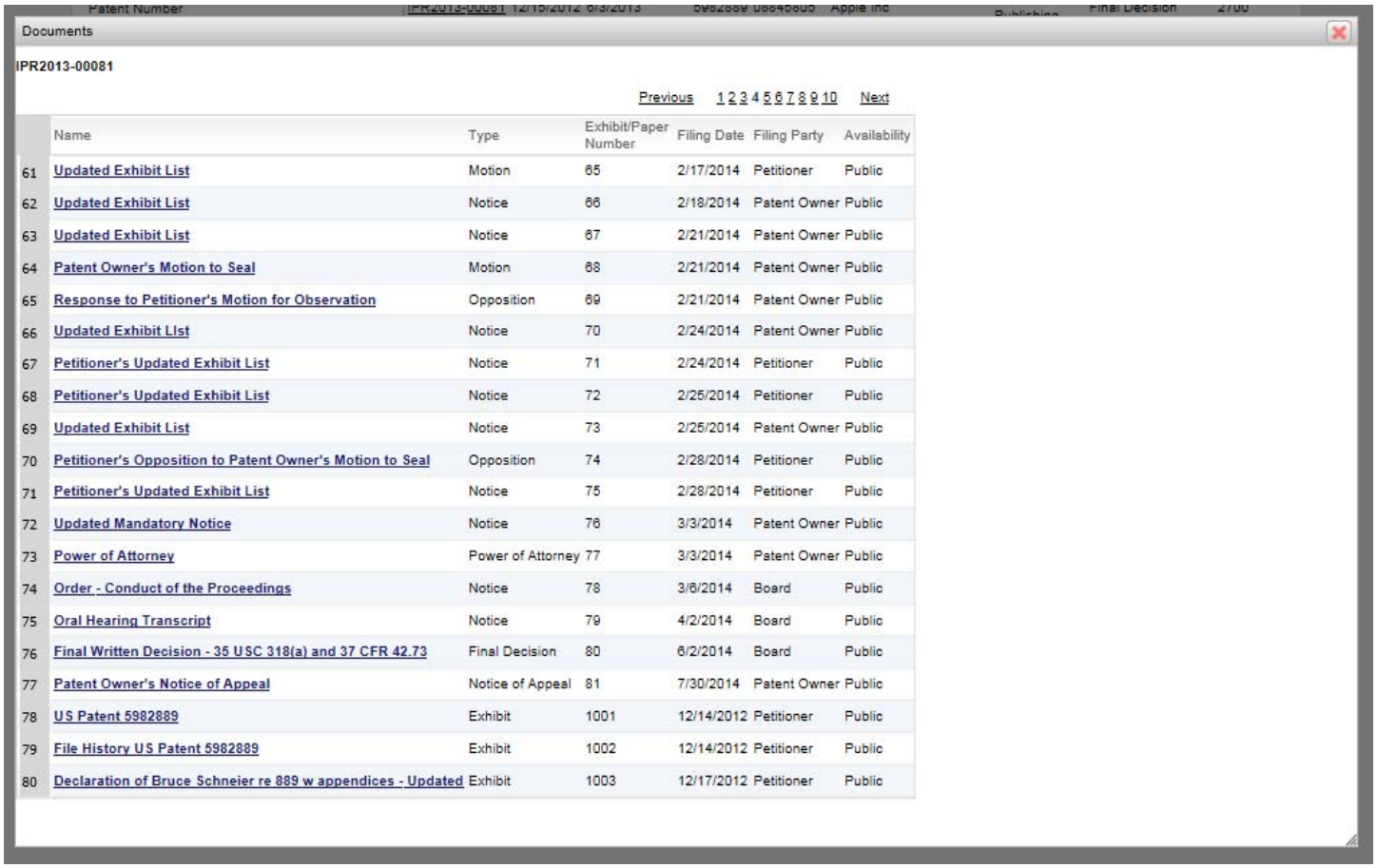
Patent Number	IPR2013-00081	12/15/2012	6/3/2013	5982889	08845805	Apple Inc	Reference Publication	Final Decision	2700

Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
41	Updated Exhibit List	Notice	44	1/2/2014	Patent Owner	Public
42	Petitioner's Motion for Additional Discovery of Certain Expert Communications	Motion	45	1/3/2014	Petitioner	Public
43	Updated Exhibit List	Notice	46	1/10/2014	Patent Owner	Public
44	Updated Exhibit List	Notice	47	1/11/2014	Patent Owner	Public
45	Patent Owner Response to MTN for Add'l Discovery re expert communications	Opposition	48	1/13/2014	Patent Owner	Public
46	Petitioner's Reply to Patent Owner's Opposition	Reply	49	1/13/2014	Petitioner	Public
47	Petitioner's REsponse to Patent Owner Statement of Facts	Reply	50	1/13/2014	Petitioner	Public
48	Updated Exhibit List	Notice	51	1/13/2014	Petitioner	Public
49	Order - Conduct of the Proceedings	Notice	52	1/21/2014	Board	Public
50	Updated Exhibit List	Notice	53	1/27/2014	Patent Owner	Public
51	Petitioner's Request for Oral Argument	Notice	54	1/29/2014	Petitioner	Public
52	Patent Owner Request for Oral Hearing	Notice	56	1/29/2014	Patent Owner	Public
53	Motion to Exclude	Notice	57	1/29/2014	Patent Owner	Public
54	Decision - Petitioner's Motion for Additional Discovery - 37 CFR 42.51(b)(2)	Notice	58	1/31/2014	Board	Public
55	ORDER Trial Hearing	Notice	59	2/3/2014	Board	Public
56	Order - Conduct of the Proceedings	Notice	60	2/4/2014	Board	Public
57	Petitioner Opposition to Motion to Exclude	Opposition	61	2/5/2014	Petitioner	Public
58	Reply to Motion to Exclude	Reply	62	2/12/2014	Patent Owner	Public
59	Order - Conduct of the Proceedings	Notice	63	2/12/2014	Board	Public
60	Petitioner's Motion for Observation on Expert Communications	Motion	64	2/17/2014	Petitioner	Public

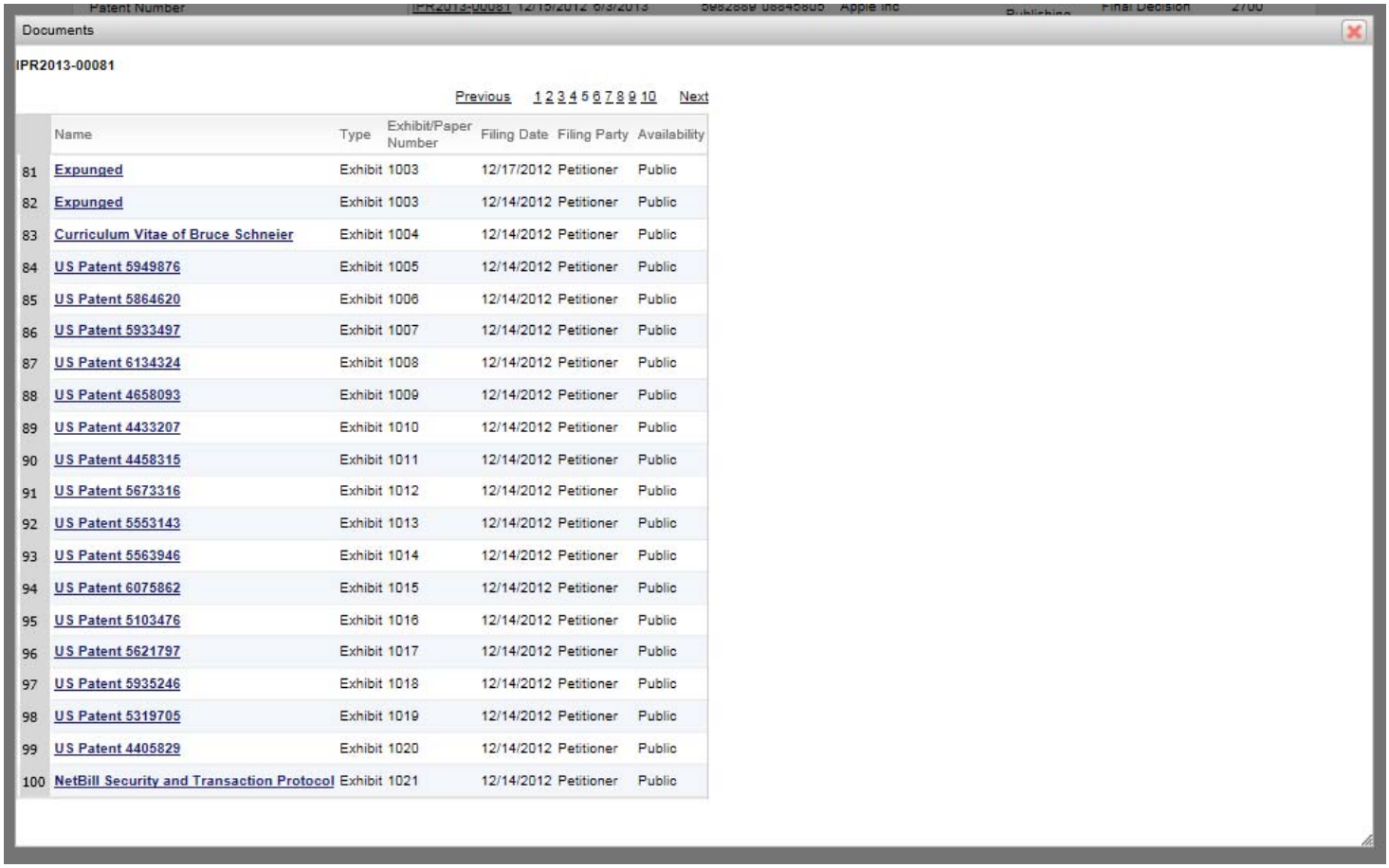


Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
61	Updated Exhibit List	Motion	65	2/17/2014	Petitioner	Public
62	Updated Exhibit List	Notice	66	2/18/2014	Patent Owner	Public
63	Updated Exhibit List	Notice	67	2/21/2014	Patent Owner	Public
64	Patent Owner's Motion to Seal	Motion	68	2/21/2014	Patent Owner	Public
65	Response to Petitioner's Motion for Observation	Opposition	69	2/21/2014	Patent Owner	Public
66	Updated Exhibit LIst	Notice	70	2/24/2014	Patent Owner	Public
67	Petitioner's Updated Exhibit List	Notice	71	2/24/2014	Petitioner	Public
68	Petitioner's Updated Exhibit List	Notice	72	2/25/2014	Petitioner	Public
69	Updated Exhibit List	Notice	73	2/25/2014	Patent Owner	Public
70	Petitioner's Opposition to Patent Owner's Motion to Seal	Opposition	74	2/28/2014	Petitioner	Public
71	Petitioner's Updated Exhibit List	Notice	75	2/28/2014	Petitioner	Public
72	Updated Mandatory Notice	Notice	76	3/3/2014	Patent Owner	Public
73	Power of Attorney	Power of Attorney	77	3/3/2014	Patent Owner	Public
74	Order - Conduct of the Proceedings	Notice	78	3/6/2014	Board	Public
75	Oral Hearing Transcript	Notice	79	4/2/2014	Board	Public
76	Final Written Decision - 35 USC 318(a) and 37 CFR 42.73	Final Decision	80	6/2/2014	Board	Public
77	Patent Owner's Notice of Appeal	Notice of Appeal	81	7/30/2014	Patent Owner	Public
78	US Patent 5982889	Exhibit	1001	12/14/2012	Petitioner	Public
79	File History US Patent 5982889	Exhibit	1002	12/14/2012	Petitioner	Public
80	Declaration of Bruce Schneier re 889 w appendices - Updated	Exhibit	1003	12/17/2012	Petitioner	Public



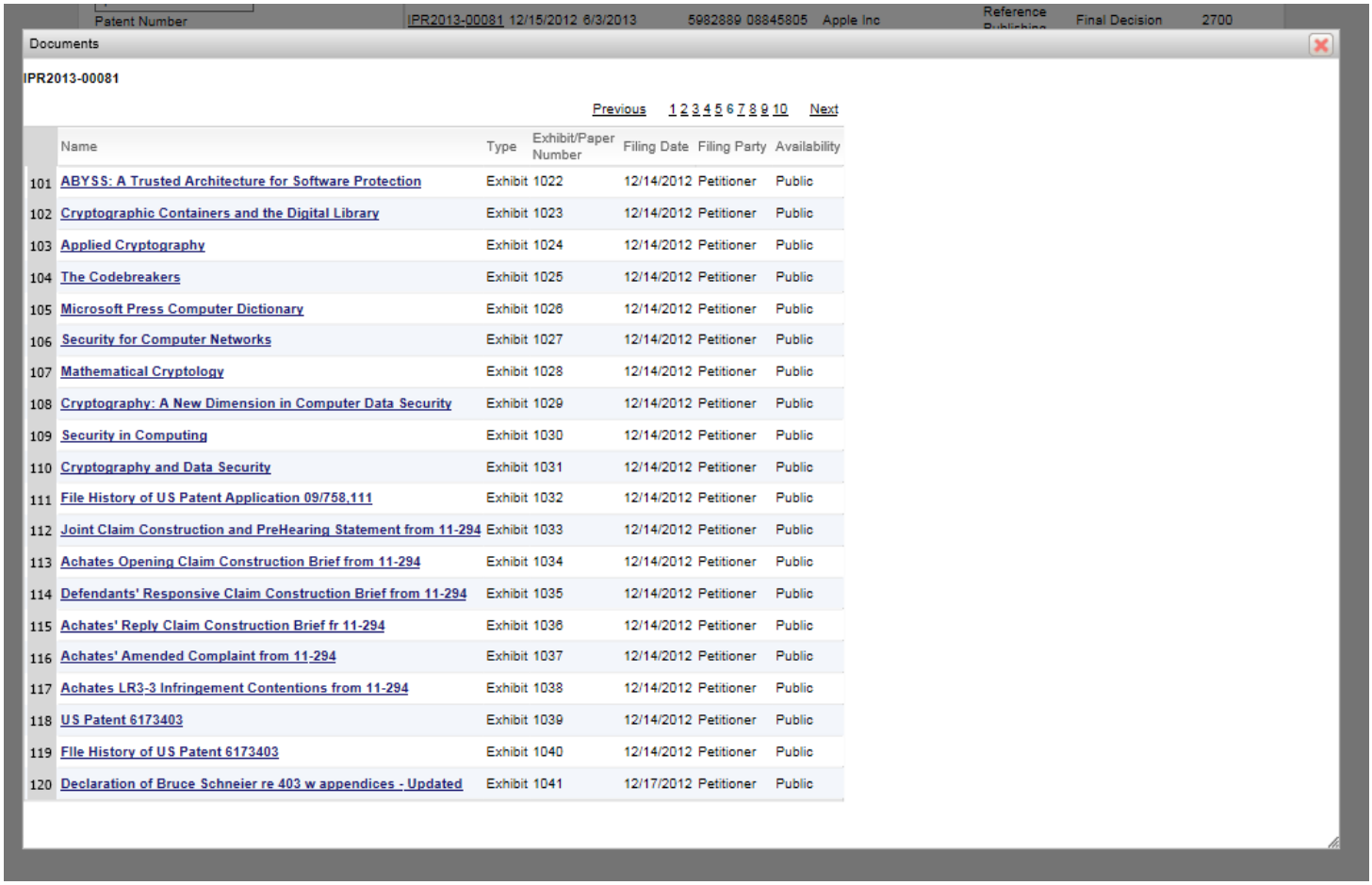
Patent Number | IPR2013-00081 12/15/2012 6/3/2013 | Apple Inc | Final Decision

Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
81	Expunged	Exhibit	1003	12/17/2012	Petitioner	Public
82	Expunged	Exhibit	1003	12/14/2012	Petitioner	Public
83	Curriculum Vitae of Bruce Schneier	Exhibit	1004	12/14/2012	Petitioner	Public
84	US Patent 5949876	Exhibit	1005	12/14/2012	Petitioner	Public
85	US Patent 5864620	Exhibit	1006	12/14/2012	Petitioner	Public
86	US Patent 5933497	Exhibit	1007	12/14/2012	Petitioner	Public
87	US Patent 6134324	Exhibit	1008	12/14/2012	Petitioner	Public
88	US Patent 4658093	Exhibit	1009	12/14/2012	Petitioner	Public
89	US Patent 4433207	Exhibit	1010	12/14/2012	Petitioner	Public
90	US Patent 4458315	Exhibit	1011	12/14/2012	Petitioner	Public
91	US Patent 5673316	Exhibit	1012	12/14/2012	Petitioner	Public
92	US Patent 5553143	Exhibit	1013	12/14/2012	Petitioner	Public
93	US Patent 5563946	Exhibit	1014	12/14/2012	Petitioner	Public
94	US Patent 6075862	Exhibit	1015	12/14/2012	Petitioner	Public
95	US Patent 5103476	Exhibit	1016	12/14/2012	Petitioner	Public
96	US Patent 5621797	Exhibit	1017	12/14/2012	Petitioner	Public
97	US Patent 5935246	Exhibit	1018	12/14/2012	Petitioner	Public
98	US Patent 5319705	Exhibit	1019	12/14/2012	Petitioner	Public
99	US Patent 4405829	Exhibit	1020	12/14/2012	Petitioner	Public
100	NetBill Security and Transaction Protocol	Exhibit	1021	12/14/2012	Petitioner	Public



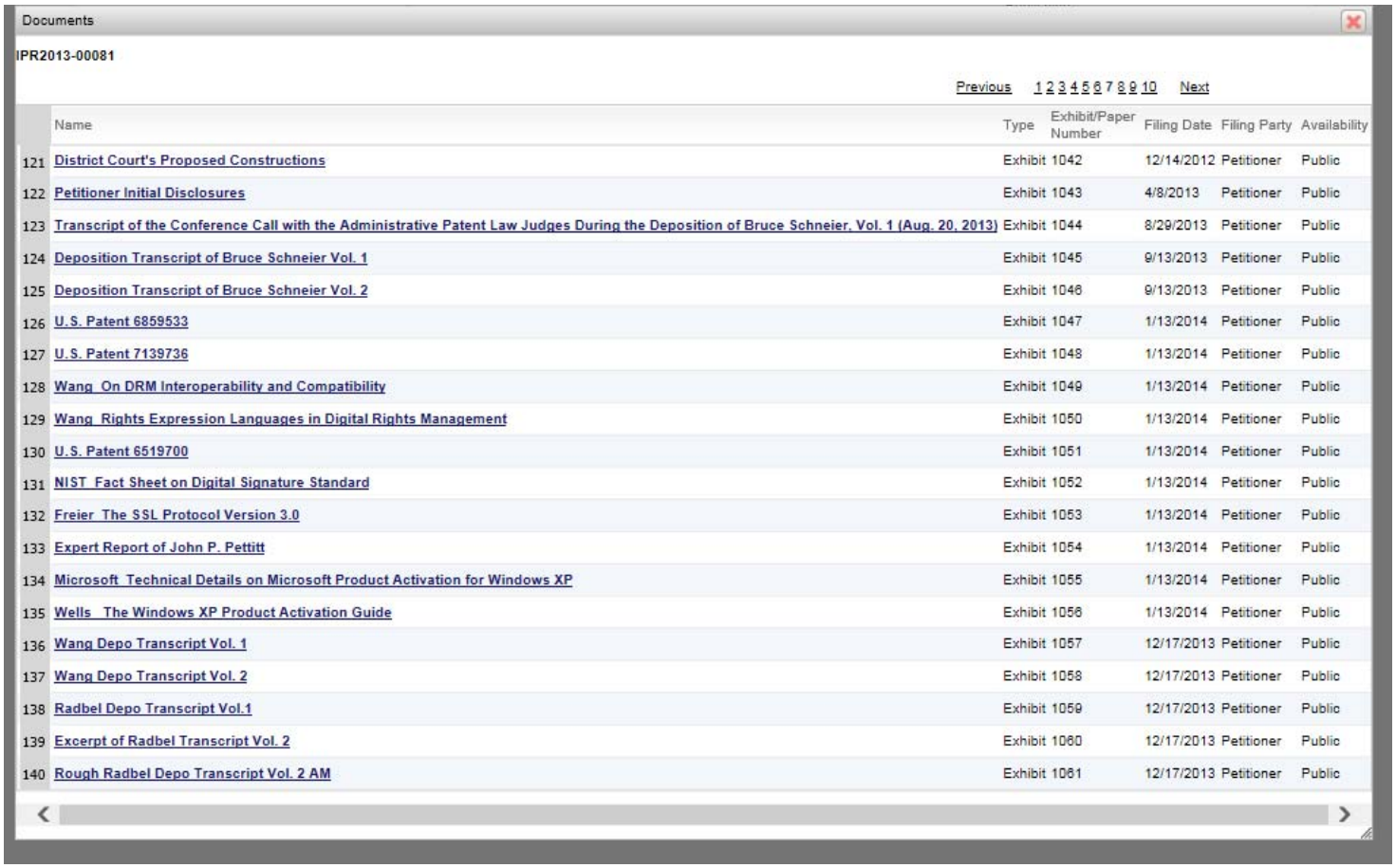
Patent Number | IPR2013-00081 | 12/15/2012 | 6/3/2013 | 5982889 | 08845805 | Apple Inc | Reference | Final Decision | 2700

Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
101	ABYSS: A Trusted Architecture for Software Protection	Exhibit	1022	12/14/2012	Petitioner	Public
102	Cryptographic Containers and the Digital Library	Exhibit	1023	12/14/2012	Petitioner	Public
103	Applied Cryptography	Exhibit	1024	12/14/2012	Petitioner	Public
104	The Codebreakers	Exhibit	1025	12/14/2012	Petitioner	Public
105	Microsoft Press Computer Dictionary	Exhibit	1026	12/14/2012	Petitioner	Public
106	Security for Computer Networks	Exhibit	1027	12/14/2012	Petitioner	Public
107	Mathematical Cryptology	Exhibit	1028	12/14/2012	Petitioner	Public
108	Cryptography: A New Dimension in Computer Data Security	Exhibit	1029	12/14/2012	Petitioner	Public
109	Security in Computing	Exhibit	1030	12/14/2012	Petitioner	Public
110	Cryptography and Data Security	Exhibit	1031	12/14/2012	Petitioner	Public
111	File History of US Patent Application 09/758,111	Exhibit	1032	12/14/2012	Petitioner	Public
112	Joint Claim Construction and PreHearing Statement from 11-294	Exhibit	1033	12/14/2012	Petitioner	Public
113	Achates Opening Claim Construction Brief from 11-294	Exhibit	1034	12/14/2012	Petitioner	Public
114	Defendants' Responsive Claim Construction Brief from 11-294	Exhibit	1035	12/14/2012	Petitioner	Public
115	Achates' Reply Claim Construction Brief fr 11-294	Exhibit	1036	12/14/2012	Petitioner	Public
116	Achates' Amended Complaint from 11-294	Exhibit	1037	12/14/2012	Petitioner	Public
117	Achates LR3-3 Infringement Contentions from 11-294	Exhibit	1038	12/14/2012	Petitioner	Public
118	US Patent 6173403	Exhibit	1039	12/14/2012	Petitioner	Public
119	FIle History of US Patent 6173403	Exhibit	1040	12/14/2012	Petitioner	Public
120	Declaration of Bruce Schneier re 403 w appendices - Updated	Exhibit	1041	12/17/2012	Petitioner	Public

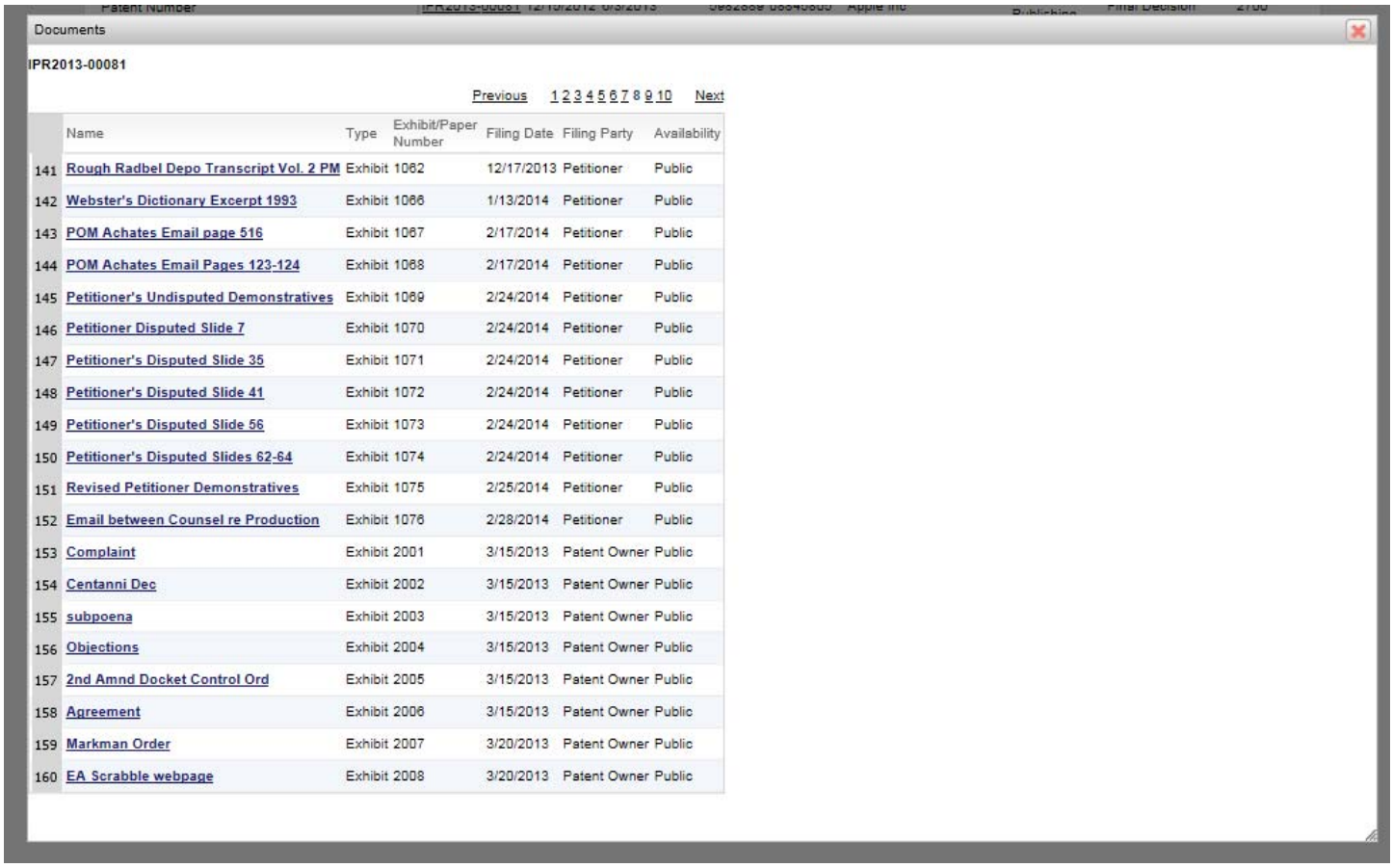


Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
121	District Court's Proposed Constructions	Exhibit	1042	12/14/2012	Petitioner	Public
122	Petitioner Initial Disclosures	Exhibit	1043	4/8/2013	Petitioner	Public
123	Transcript of the Conference Call with the Administrative Patent Law Judges During the Deposition of Bruce Schneier, Vol. 1 (Aug. 20, 2013)	Exhibit	1044	8/29/2013	Petitioner	Public
124	Deposition Transcript of Bruce Schneier Vol. 1	Exhibit	1045	9/13/2013	Petitioner	Public
125	Deposition Transcript of Bruce Schneier Vol. 2	Exhibit	1046	9/13/2013	Petitioner	Public
126	U.S. Patent 6859533	Exhibit	1047	1/13/2014	Petitioner	Public
127	U.S. Patent 7139736	Exhibit	1048	1/13/2014	Petitioner	Public
128	Wang On DRM Interoperability and Compatibility	Exhibit	1049	1/13/2014	Petitioner	Public
129	Wang Rights Expression Languages in Digital Rights Management	Exhibit	1050	1/13/2014	Petitioner	Public
130	U.S. Patent 6519700	Exhibit	1051	1/13/2014	Petitioner	Public
131	NIST Fact Sheet on Digital Signature Standard	Exhibit	1052	1/13/2014	Petitioner	Public
132	Freier The SSL Protocol Version 3.0	Exhibit	1053	1/13/2014	Petitioner	Public
133	Expert Report of John P. Pettitt	Exhibit	1054	1/13/2014	Petitioner	Public
134	Microsoft Technical Details on Microsoft Product Activation for Windows XP	Exhibit	1055	1/13/2014	Petitioner	Public
135	Wells The Windows XP Product Activation Guide	Exhibit	1056	1/13/2014	Petitioner	Public
136	Wang Depo Transcript Vol. 1	Exhibit	1057	12/17/2013	Petitioner	Public
137	Wang Depo Transcript Vol. 2	Exhibit	1058	12/17/2013	Petitioner	Public
138	Radbel Depo Transcript Vol.1	Exhibit	1059	12/17/2013	Petitioner	Public
139	Excerpt of Radbel Transcript Vol. 2	Exhibit	1060	12/17/2013	Petitioner	Public
140	Rough Radbel Depo Transcript Vol. 2 AM	Exhibit	1061	12/17/2013	Petitioner	Public

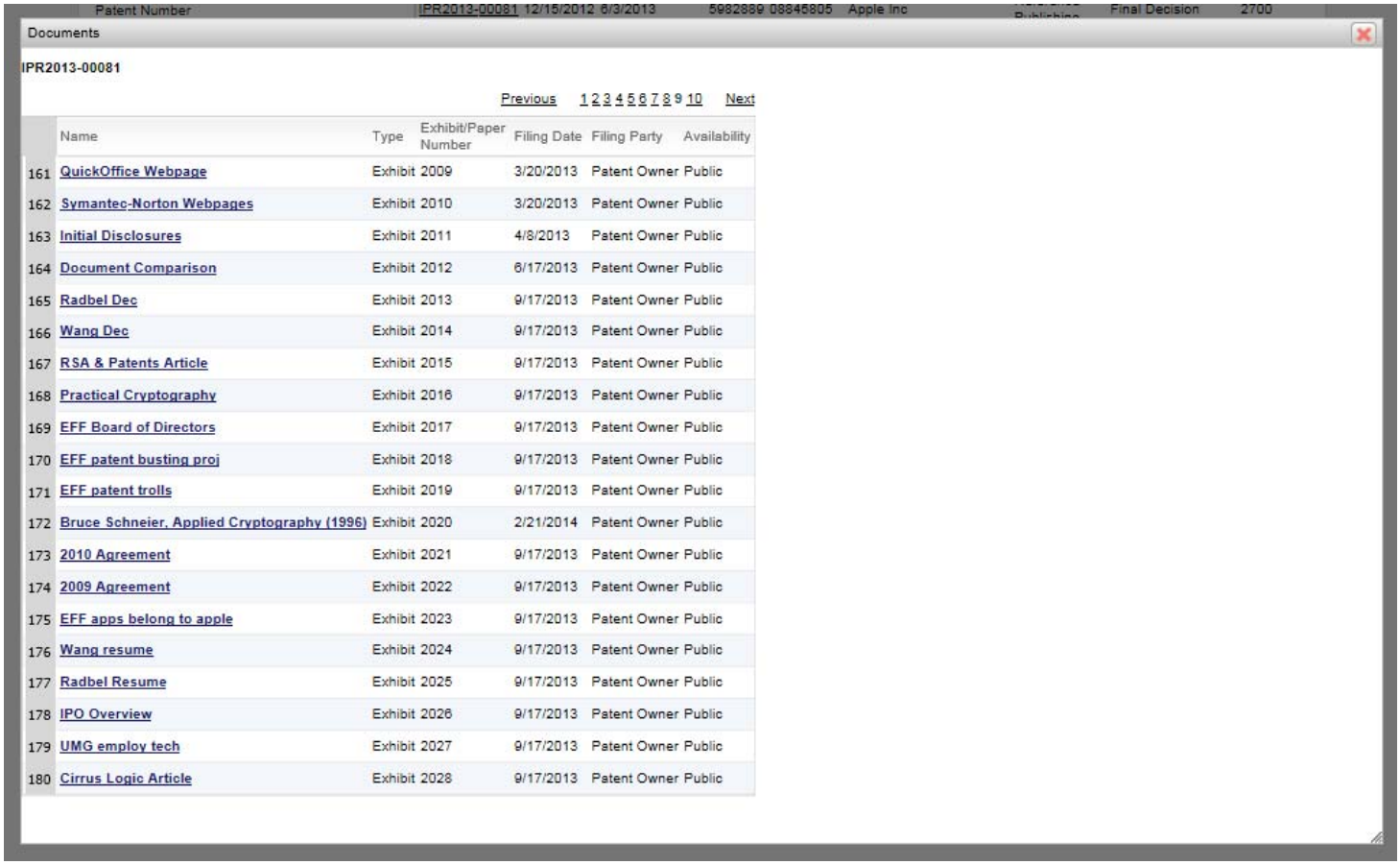


Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
141	Rough Radbel Depo Transcript Vol. 2 PM	Exhibit	1062	12/17/2013	Petitioner	Public
142	Webster's Dictionary Excerpt 1993	Exhibit	1066	1/13/2014	Petitioner	Public
143	POM Achates Email page 516	Exhibit	1067	2/17/2014	Petitioner	Public
144	POM Achates Email Pages 123-124	Exhibit	1068	2/17/2014	Petitioner	Public
145	Petitioner's Undisputed Demonstratives	Exhibit	1069	2/24/2014	Petitioner	Public
146	Petitioner Disputed Slide 7	Exhibit	1070	2/24/2014	Petitioner	Public
147	Petitioner's Disputed Slide 35	Exhibit	1071	2/24/2014	Petitioner	Public
148	Petitioner's Disputed Slide 41	Exhibit	1072	2/24/2014	Petitioner	Public
149	Petitioner's Disputed Slide 56	Exhibit	1073	2/24/2014	Petitioner	Public
150	Petitioner's Disputed Slides 62-64	Exhibit	1074	2/24/2014	Petitioner	Public
151	Revised Petitioner Demonstratives	Exhibit	1075	2/25/2014	Petitioner	Public
152	Email between Counsel re Production	Exhibit	1076	2/28/2014	Petitioner	Public
153	Complaint	Exhibit	2001	3/15/2013	Patent Owner	Public
154	Centanni Dec	Exhibit	2002	3/15/2013	Patent Owner	Public
155	subpoena	Exhibit	2003	3/15/2013	Patent Owner	Public
156	Objections	Exhibit	2004	3/15/2013	Patent Owner	Public
157	2nd Amnd Docket Control Ord	Exhibit	2005	3/15/2013	Patent Owner	Public
158	Agreement	Exhibit	2006	3/15/2013	Patent Owner	Public
159	Markman Order	Exhibit	2007	3/20/2013	Patent Owner	Public
160	EA Scrabble webpage	Exhibit	2008	3/20/2013	Patent Owner	Public



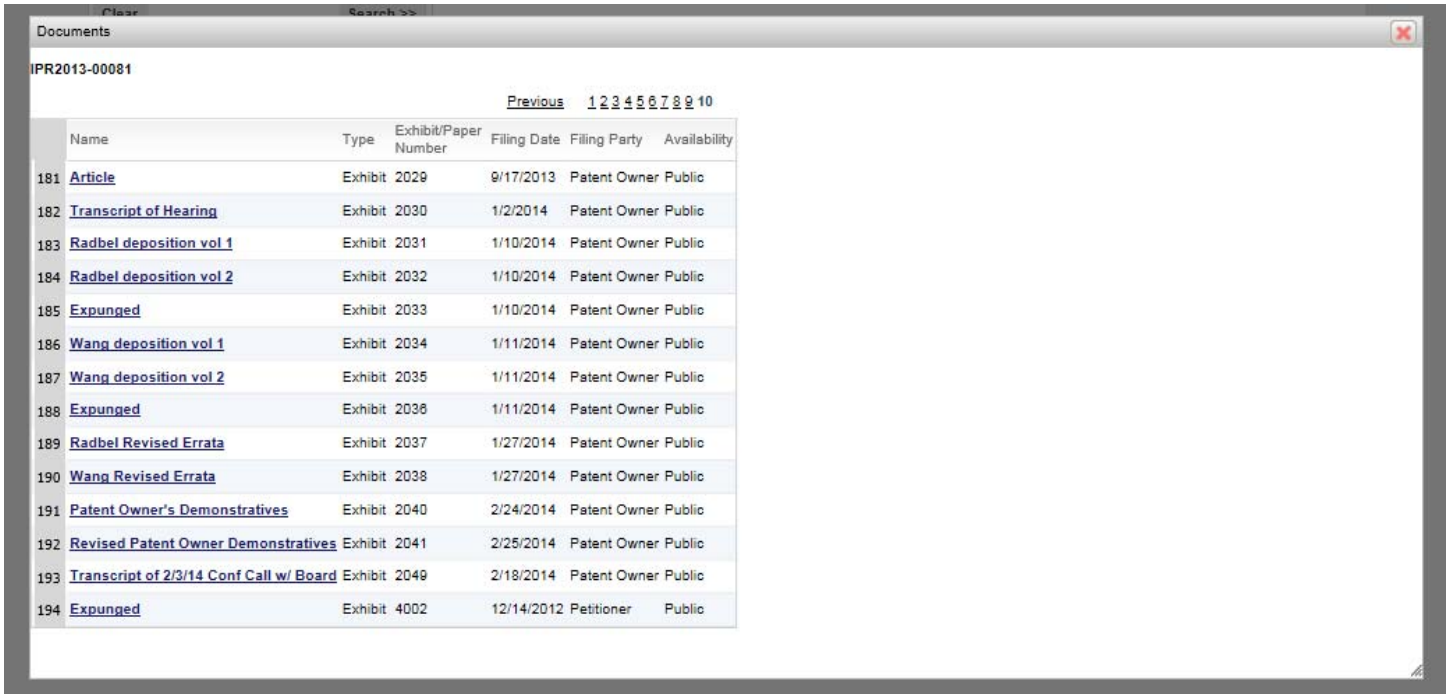
Patent Number | IPR2013-00081 | 12/15/2012 | 6/3/2013 | 5982889 | 08846805 | Apple Inc | Final Decision | 2700

Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10 Next

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
161	QuickOffice Webpage	Exhibit	2009	3/20/2013	Patent Owner	Public
162	Symantec-Norton Webpages	Exhibit	2010	3/20/2013	Patent Owner	Public
163	Initial Disclosures	Exhibit	2011	4/8/2013	Patent Owner	Public
164	Document Comparison	Exhibit	2012	6/17/2013	Patent Owner	Public
165	Radbel Dec	Exhibit	2013	9/17/2013	Patent Owner	Public
166	Wang Dec	Exhibit	2014	9/17/2013	Patent Owner	Public
167	RSA & Patents Article	Exhibit	2015	9/17/2013	Patent Owner	Public
168	Practical Cryptography	Exhibit	2016	9/17/2013	Patent Owner	Public
169	EFF Board of Directors	Exhibit	2017	9/17/2013	Patent Owner	Public
170	EFF patent busting proj	Exhibit	2018	9/17/2013	Patent Owner	Public
171	EFF patent trolls	Exhibit	2019	9/17/2013	Patent Owner	Public
172	Bruce Schneier, Applied Cryptography (1996)	Exhibit	2020	2/21/2014	Patent Owner	Public
173	2010 Agreement	Exhibit	2021	9/17/2013	Patent Owner	Public
174	2009 Agreement	Exhibit	2022	9/17/2013	Patent Owner	Public
175	EFF apps belong to apple	Exhibit	2023	9/17/2013	Patent Owner	Public
176	Wang resume	Exhibit	2024	9/17/2013	Patent Owner	Public
177	Radbel Resume	Exhibit	2025	9/17/2013	Patent Owner	Public
178	IPO Overview	Exhibit	2026	9/17/2013	Patent Owner	Public
179	UMG employ tech	Exhibit	2027	9/17/2013	Patent Owner	Public
180	Cirrus Logic Article	Exhibit	2028	9/17/2013	Patent Owner	Public



Documents

IPR2013-00081

Previous 1 2 3 4 5 6 7 8 9 10

	Name	Type	Exhibit/Paper Number	Filing Date	Filing Party	Availability
181	Article	Exhibit	2029	9/17/2013	Patent Owner	Public
182	Transcript of Hearing	Exhibit	2030	1/2/2014	Patent Owner	Public
183	Radbel deposition vol 1	Exhibit	2031	1/10/2014	Patent Owner	Public
184	Radbel deposition vol 2	Exhibit	2032	1/10/2014	Patent Owner	Public
185	Expunged	Exhibit	2033	1/10/2014	Patent Owner	Public
186	Wang deposition vol 1	Exhibit	2034	1/11/2014	Patent Owner	Public
187	Wang deposition vol 2	Exhibit	2035	1/11/2014	Patent Owner	Public
188	Expunged	Exhibit	2036	1/11/2014	Patent Owner	Public
189	Radbel Revised Errata	Exhibit	2037	1/27/2014	Patent Owner	Public
190	Wang Revised Errata	Exhibit	2038	1/27/2014	Patent Owner	Public
191	Patent Owner's Demonstratives	Exhibit	2040	2/24/2014	Patent Owner	Public
192	Revised Patent Owner Demonstratives	Exhibit	2041	2/25/2014	Patent Owner	Public
193	Transcript of 2/3/14 Conf Call w/ Board	Exhibit	2049	2/18/2014	Patent Owner	Public
194	Expunged	Exhibit	4002	12/14/2012	Petitioner	Public